Facultad de Ingeniería

Carrera de Ingeniería de Sistemas e Informática

“Implementación de un Sistema de Monitoreo Para Asegurar la Continuidad de los Servicios en un Data Center Utilizando Protocolo SNMP”

Autor: Oré Alvaro Cristian

Para obtener el Título Profesional de
Ingeniero de Sistemas e Informática

Asesor: Molina Velarde Pedro

Lima, Junio 2019

DEDICATORIA

Agradezco principalmente a Dios por brindarme vida, fuerza y salud para continuar con mis objetivos, a mi mamá por ofrecerme siempre su apoyo absoluto y a mi hijo por ser mi mayor inspiración día a día.

RESUMEN EJECUTIVO

El presente trabajo se origina como una necesidad primordial de contar con un sistema de monitoreo para toda la infraestructura del Data Center en la empresa Netsecure Perú, debido que al transcurrir los años la empresa ha ido incrementando sus servicios y equipos tecnológicos, teniendo una función primordial para las empresas debido a que brindar y entregar información de valor a todos sus clientes.

La constante batalla que deben librar la organización es que sus servicios estén disponibles las 24 horas los 7 días de la semana; tomando en cuenta siempre que estos sean de excelente calidad, eficientes y oportunos. Para ello es significativo conocer el estado de los procedimientos que se utilizan dentro de la organización que permitan certificar la correcta ejecución de los mismos, es ineludible que estos sistemas se conserven prestando el servicio el mayor tiempo posible y sin interrupciones, si existiera una situación inusual, como podría ser el caso cuando un servidor se quede sin suministro de energía eléctrica, exceso de sobrecarga de CPU, Memoria y Capacidad, condiciones ambientales de temperatura mayor a los 27° C, reinicio automático de servicios, incremento de las conexiones a Internet debido a un buen uso del ancho de banda la cual nos podría indicar un potencial ataque. De esta manera, tendrá que notificar al Ingeniero a cargo para que pueda actuar de manera proactiva a fin de evitar una negativa en los servicios o extravío de información.

Es esencial mostrar que todos los servicios se mantienen en constante monitoreo, y así exaltar el prestigio con la clientela, para ello es importante contar con una buena herramienta de monitoreo, el cual sea competente de avisar sobre errores en la red y exponer su actuación mediante el examen de tráfico. Es de relevancia que estas advertencias sean muy honestas ya que si se reportara aparentes alarmas el sistema perdería prestigio y credibilidad.

El esquema de monitorización propuesto pretende informar la correcta actuación de la red, los servidores y servicios, el cual se halla orientado a desplegarse en una de la compañía más prestigiosa en el ambiente de la tecnología de la informática Netsecure Perú

Debido a esto, el presente proyecto muestra la implementación de un sistema de monitoreo utilizando el protocolo Simple Network Management Protocol (SNMP), que nos va permitir ayudar a monitorear de manera eficiente, y ser capaz de resolver incidencias de forma rápida y, más que eso, ser capaz de anticiparse en la prevención de situaciones críticas de extrema relevancia, con el propósito de asegurar la continuidad de la operación de los recursos de TI sin afectar los procesos de negocio. El seguimiento de algunos indicadores puede ayudar mucho en una acción proactiva para el equipo de TI, ayuda a descubrir los problemas y evita antes de que estas sucedan. Minutos de interrupción puede costar muy caro a la organización.

INDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCION

En adelante, se circunscribe una investigación enfocada en el desarrollo de nuevas tecnologías, enmarcada en el contexto de una de las empresas más prestigiosa del país, en materia tecnológica, con la finalidad de otorgar a través de este proyecto, un caudal de información, proclive no solo a mejorar la eficiencia de la misma, sino capaz de proteger los datos de servicios y de funcionamiento de esta Empresa.

Cabe señalar que, el trabajo de vigilancia de redes monitoreo y servicios es de gran relevancia para esta empresa, porque depende de esto la comprensión del funcionamiento frecuente de su estructura de comunicaciones. Por ello, se planteó a Netsecure Perú la idea de la implementación de un sistema de monitorización para resguardar la prolongación de los servicios, avalando de éste modo la prestación de un servicio competitivo y muy calificado, perdurable en el tiempo.

Por lo que, se muestra un compendio documental de tipo informativo correspondiente a la implementación de un sistema de monitorización para asegurar la prolongación de los servicios utilizados en un Data Center utilizando protocolo SNMP para la organización Netsecure Perú, en que se incluye una explicación de los diversos patrones de gestión de red, una síntesis de las formalidades y sistemas considerablemente usadas por otras empresas para el monitoreo y servicio de su estructura de tecnología, aunado a otros datos relacionados.

En forma general lo que pretende la gestión de red es disminuir los riesgos frente a una posible falla en el manejo de datos informativos, minimizar los costos y evitar que suceda algún contratiempo y sobre todo mantener la red en funcionamiento brindando servicios eficientes y oportunos. Las herramientas de gestión de red se pueden ver como un elemento de seguridad en la red, ya que manejan información sobre el ejercicio de los equipos y pueden prevenir problemas a futuro, en otras palabras, fortalecen la disponibilidad de los servicios.

En líneas generales, para hacer de esta una investigación comprensible, se procedió a desarrollar una estructura de cuatro capítulos, los cuales se referencian en un orden especifico, iniciando con el capítulo I inherente a los aspectos generales el cual ofrece elementos básicos para reconocer y llevar a cabo la investigación; posteriormente se desarrolló el capítulo II relativo al fundamento teórico, que facilita la comprensión de los aspectos tomados en cuenta para la obtención de la misma, luego se tiene el capítulo III dedicado al desarrollo del proyecto, en el que destaca la propuesta hecha a la empresa y por último el capítulo IV reservado para el análisis de costos y beneficios en el cual se demuestra la factibilidad de esta investigación.

Es necesario mencionar que esta se ejecutó mediante un diseño cuasi experimental de campo con una tipología descriptiva, enmarcado de una modalidad factible, con un nivel proyectivo y explicativo, con apoyo del método empírico como técnica de recolección de la información y la encuesta, lo cual facilito la recolección y la organización de la información que dio pie al desarrollo de esta propuesta.

CAPITULO 1: ASPECTOS GENERALES

1.1. Ámbito de Estudio

Con relación al contexto de investigación, se puede explicar que, se halla orientado a efectuar un análisis e implementación de la herramienta PRTG la cual consiente en realizar el monitoreo del estado actual de la red y así poder asegurar la continuidad de los servicios utilizados en un Data Center utilizando protocolo SNMP para la Empresa Netsecure Perú, hoy en día la dirección de TI posee un checklist o sistema de monitoreo en los servidores cuya función es esencial puesto que en estas hay albergados productos en los cuales se organizan, protegen y gestionan la información de los clientes y de la empresa en sí. Para una mayor comprensión de su entorno es importante observar su distribución organizativa, tal y como se muestra en la figura 1:

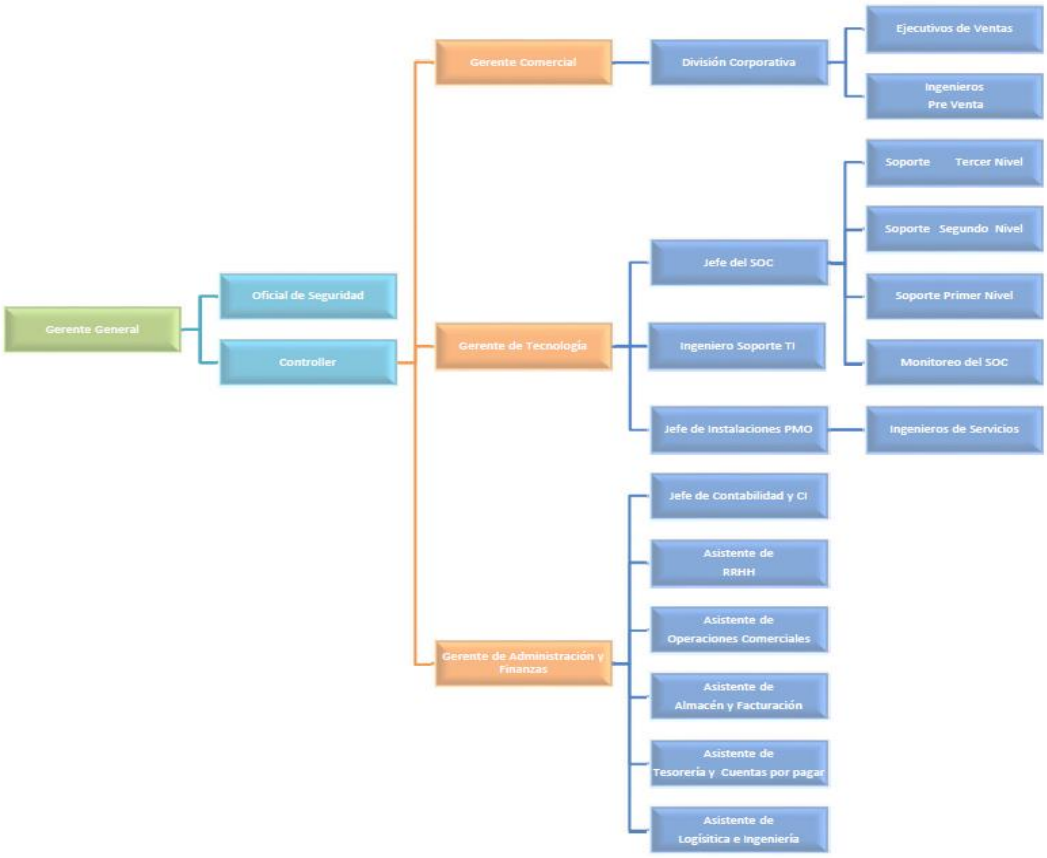

Figura 1: Organigrama de la Empresa

***Fuente**: Netsecure (2019)*

1.2. Descripción Actual del negocio

Netsecure Perú Informática cuenta con más de 2 décadas en la práctica Seguridad de la Información, ofreciendo una amplia gama de atención y servicios en el ramo, trabajando con marcas reconocidas en el medio, entre ellas son Fortinet, Aruba, Imperva, CheckPoint, F5, Fireeye, Infoblox, Intel Security McAfee y Allot. Ofrecen asesoría general sobre el uso y en materia de resolución de conflictos en el área. Brindando atención eficiente dirigida a subsanar las insuficiencias en Seguridad de la Información de sus consumidores y generar relaciones a largo plazo.

Asimismo, NetSecure se encuentra trabajando en alianzas comerciales en todo el país por más de dos décadas. Asumiendo en primera instancia la capacidad de facilitar y procurar un servicio de alta particularidad encaminados a compensar los requerimientos informáticos de sus clientes para posicionarse con ellos en el tiempo como una de las mejores empresas en este ámbito.

De allí que, la principal función es la composición de procedimientos de seguridad informática, siendo estos la fortaleza en la que NetSecure posee la más alta determinación profesional para desplegar toda clase de proyecciones, comprendiendo todos los elementos implicados o la localización del problema que presente el cliente, o reingeniería o adelanto de la Solución o Suministro de hardware y software o Establecimiento y puesta en marcha o mantenimiento preventivo correctivo, monitoreo, administración, o simplemente capacitación.

Netsecure es una Multinacional de Tecnología, Servicios y Consultoría en Seguridad de la Información cuenta con alrededor de 200 Profesionales que participan en sus 5 sedes localizadas en Perú, Chile, Colombia, Ecuador y EEUU (Netsecure, 2019, p. 23).

Servicios Gestionados:

Según Netsecure (2019) son los siguientes:

- Prontas respuestas que aseguran la continuidad del negocio, el acceso a las aplicaciones, y la capacidad de la red tanto la oficina principal como instalaciones remotas y distribuidas.
- Seguridad contra amenazas concertadas y ataques no identificados.
- Evitar constantes aumentos en personal de seguridad para seleccionar, desplegar y administrar soluciones de seguridad.
- Soluciones de administración escalable, que contribuyan a la eficiencia y al cumplimiento de nuevas regulaciones.
- Disminuir los costos de adquisición, administración asociados a las funciones de seguridad e instalación.
- Obtener la mejor seguridad, pero al mismo tiempo disminuir el número de distribuidores.
- Esquema de inversión flexible que permita adquirir lo que necesita hoy y expandirse más tarde.
- Fundar, efectuar, y mantener una política de seguridad corporativa.
- Productos de Seguridad Gestionados
- Incorporamos en su Red las funcionalidades de seguridad que su empresa requiere (Firewall, Filtro Contenido, Correo, Antivirus, Antispam, IDS/IPS, VPN, otros). Desde el SOC de la organización, estas unidades serán:

    1. El Monitoreado 7x24 este monitoreo puede ser primordial para lograr la continuidad operativa de su centro de datos, debido a que permite prevenir fallas y mejorar las operaciones, por ello al escoger este tipo de herramienta, se debe evaluar que brinde claridad sobre el estado del centro de datos; que reduzca la paralización del servicio; y merme el tiempo de tipificación de fallas; que opere 24x7 en línea; reduciendo el costo de operaciones del centro de datos.

Queda claro, que ningún instrumento es suficiente si no se tienen los debidos procedimientos internos para resolver las situaciones que se presentan con la información obtenida.

2. Los servicios Administrados son los que garantizan la disponibilidad, confiabilidad y desempeño del sistema de monitoreo a través de los servicios profesionales que se ofrecen.
3. En relación a los respaldados en cuanto a configuración y políticas las empresas que prestan los servicios de monitoreo hacen una copia de seguridad o respaldo de los datos que parezcan vulnerables en caso de software dañado o defectuoso, descomposición de datos, falla de hardware, piratería (*hacking*), error de usuario u otros contratiempos. Cuando se realizan las copias de seguridad capturan y sincronizan una fotografía de un aspecto en el tiempo que posteriormente se usa para devolver los datos a su estado anterior.
4. Actualizados en forma remota este aspecto tiene como objetivo de dar a conocer una mejor forma para visualizar la información sobre algún proceso a distancia en tiempo real, que puede ser aplicado en industrias o simplemente pequeñas y medianas empresas, ofreciendo una solución comparativamente más económica que los existentes en el mercado.
5. Acceso a soporte técnico especializado es un rango de servicios a través del cual se suministra apoyo a los usuarios al tener algún problema al hacer uso de un bien o servicio, bien sea, este el hardware o software de un computador de un servidor de Internet con servicio de monitoreo.

6. Prevención de intrusiones en la red esto habla sobre estos sistemas que detectan y bloquean cualquier intento de intromisión, transmisión de código malicioso o amenazas a través de la red, sin impacto alguno sobre su rendimiento.
7. Activación y generación de alertas este proceso identifica el manejo de un sistema que continuamente monitorea una red de computadores en busca de elementos dañados o maliciosos, para luego notificar al administrador de la red mediante correo electrónico u otras alarmas.
8. Análisis y evaluación de actividades sospechosas esto es una contribución inicial en una serie de valor procesal, que eventualmente serviría de insumo para un caso de investigación en dado caso de ser necesario.
9. Activación de procedimiento para manejo de Incidentes La función de la gestión de acontecimientos es recobrar el nivel usual de ejercicio del servicio y disminuir en todo lo que se pueda el aspecto perjudicial en la empresa de forma que la eficacia del servicio y la habilidad se mantengan.
10. Reportes periódicos y on-line de su servicio consiste en que se podrá visualizar online mediante un usuario y contraseña, los programas de todas las actividades y eventos que reconoce su panel de alarma y que es enviado a la central de monitoreo.
11. Mantenimiento Correctivo con tiempo de solución comprometido es un sistema que permite atender las necesidades de mantenimiento correctivo que consta en la reparación de averías de forma eficiente.

Monitoreo y Correlación

En relación con la seguridad y disposición de sus medios no debe suspenderse por los altos costos de herramientas y servicios. Netsecure ofrece una solución de Monitoreo de Seguridad y Disponibilidad, en dispositivos críticos de su organización, con el fin de brindar acceso a una amplia y sofisticada gama de mecanismos de servicio de la seguridad (SIEM) sin tener que invertir elevadas sumas de dinero ni tiempos de implementación. Al efectuar todas las soluciones, se están solventando varias necesidades que han sido detectadas en la red del cliente, por ejemplo:

- Reducir costos en la administración y troubleshooting de seguridad.
- Afirmar una rápida respuesta ante sucesos de seguridad.
- Mantener un control sobre los niveles de servicio de sus aplicaciones y sistemas críticos.
- Acumular registros auténticos para estadísticos y análisis forense.
- Ahorro en la capacidad de crecimiento a nivel de eventos por segundo, sin necesidad de comprar licencias ni Hardware adicionales.
- Coincidencia para resguardo de logos y reportes.
- Consentir escanear habitualmente los servicios web en busca de nuevas debilidades.
- Agrupar y perfeccionar los recursos a través de plataformas fortalecidas.

En tal sentido, esto daría mayor sensación de seguridad, en cuanto al manejo y revisión constante de estas herramientas de gestión.

Servicio de oficial de seguridad de la información:

En cuanto al servicio de Outsourcing de Oficial de Seguridad de la Información, consta en suministrar a los clientes, un asesor en seguridad bajo el rol de Oficial de Seguridad Interno, a través de las mejores prácticas de seguridad conseguirá aplicar y ejercer un control efectivo en materia de seguridad de la información al interior de la empresa.

Ya que una amenaza más grande de la compañía es el robo de información y los ataques cibernéticos, por lo que es importante contar con medidas que ayuden a la defensa y sobre todo concentrar en el equipo de trabajo a un Oficial de Seguridad de la Información, quien intuya la habilidad comercial y gestión de riesgos, no sólo la ciberseguridad.

Servicio de elaboración de planes de continuidad del negocio

En este sentido, la Secuencia de Negocios, dentro de las empresas debe ser tomada como una necesidad vital, dado que, a través de esta, se avala la continuidad de las operaciones frente a los obstáculos que pueden tener como causa situaciones de diferentes índoles, ya sean naturales, causados por el hombre o tecnológicos. Los planes de continuidad de negocios afirman la continuidad de los procesos del negocio tomando en cuenta a las personas y la estructura tecnológica y física.

Es importante mencionar que un plan que dé continuidad al ejercicio (BCP por sus siglas en inglés, Business Continuity Plan) son el seguro más accesible y económico que una empresa bien sea grande o pequeña logre obtener, principalmente para las compañías pequeñas, y usualmente no cuesta nada hacerlo.

Se entiende que las planificaciones de continuidad del negocio son acreditadas como Planes para Recuperación de un Desastre (DRP, Disaster Recovery Plan) y los mismos coinciden mucho. Pero, un DRP siempre tiene que estar siempre encaminado a recuperarse después de una pérdida para que el BCP muestre como prolongar el hacer

negociaciones hasta que la total recuperación sea una realidad. Juntos son de suma importancia y a menudo son combinados en un solo documento por ser más conveniente. (Valoradata, 2018)

Servicio de análisis de vulnerabilidades

Para entender este aspecto, la vulnerabilidad informática se puede pensar como una debilidad de cualquier tipo que afecta o envuelve la seguridad de un mecanismo informático. Este servicio enmarca un propósito como lo es medir el nivel de seguridad que tenga la plataforma tecnológica del beneficiario, por medio de la caracterización de las vulnerabilidades que la afectan. A través de este análisis es posible equiparar los riesgos con el potencial suficiente de afectar la confidencialidad, integridad y el disponible de la plataforma tecnológica.

Preventa; diseña y define la arquitectura de la solución: Gestión de Proyectos (PMO); inspecciona la ejecución del plan en calidad, recursos y tiempos, usando sistemáticas de última generación. Actualmente es común que la gestión en las compañías se ejecute por proyectos y no por procesos. De hecho, la gerencia de proyectos es una de las más eficaces herramientas de gestión creadas hasta la fecha. Para implementar; se cuenta con ingenieros totalmente capacitados en las tecnologías que esta empresa representa (Sáenz, A. 2012).

Centro de Capacitación: Se sabe que el adiestramiento es un proceso primordial para una compañía, porque gracias a esto, se fortifican destrezas y conocimientos en el equipo humano, asegurando así productividad y competencia dentro del mercado. En tal sentido el adiestramiento cumple una función fundamental y es de mejorar el presente y ayudar a edificar un futuro en el que la fuerza de trabajo esté constituida para superarse perennemente y esto debe realizarse como un proceso, siempre en relación con el puesto y las metas de la organización.

1.3. Definición del Problema

1.3.1 Descripción Actual

Una correcta supervisión de todos los servicios que se hallan albergados en el Data center, es una de las responsabilidades del Ingeniero de Soporte IT, y está compuesto por un solo ingeniero, ya tiene una carga considerable de trabajo debido a las múltiples tareas que debe realizar. Teniendo en cuenta que son dos sedes en las que se encuentran instalados, servidores, Router, Switch, Firewall, Antispam, Servicios Publicados, la sede Principal ubicado en San Isidro y la otra sede que se encuentra ubicado en Villa el Salvador, ya que para monitorear sobre ellos es necesario ingresar a cada una de ellas, lo cual hace que una gestión de este tipo sea prácticamente ineficiente con unos tiempos muy altos de respuesta ante eventos.

De allí que, una red lenta o de baja performance es un verdadero problema para la empresa ya que genera pérdida de productividad, identificar la raíz del problema a tiempo es muy complicado para el ingeniero a cargo. Existen varias causas para que se genere lentitud en la red, entre las más destacadas son:

- Placas de red defectuosas
- Fallas en switches o router
- Conflictos de IP
- Exceso de aplicaciones que operan sobre la red

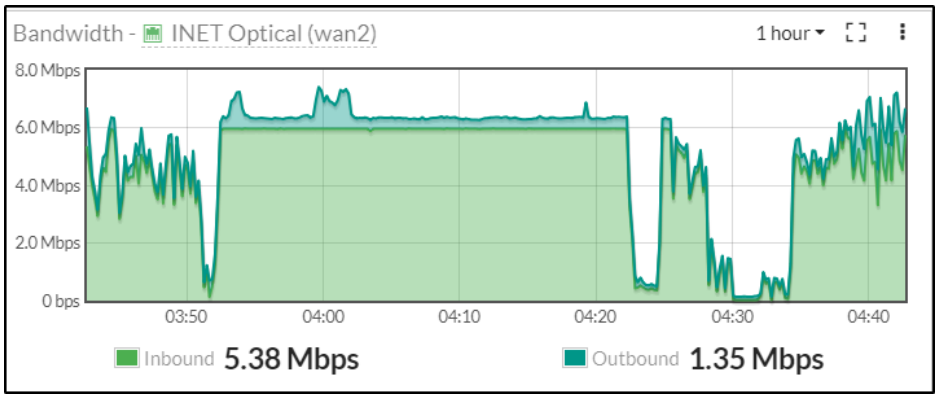

Figura 2. Causas de Lentitud en la Red

***Fuente**: Oré, C. (2019)*

Teniendo claro qué se necesita que los recursos libres de CPU y memoria para que los servidores puedan cumplir con su tarea, es de vital importancia supervisar los procesadores de estos componentes fundamentales de la red. En general, la supervisión de la CPU debe abarcar los servidores, routers, switches y equipos de seguridad que interactúan dentro de la organización. Muchos procesos innecesarios en ejecución podrían causar diversos comportamientos secundarios en la red, es de vital importancia identificar a tiempo el exceso de sobre carga de CPU y memoria.

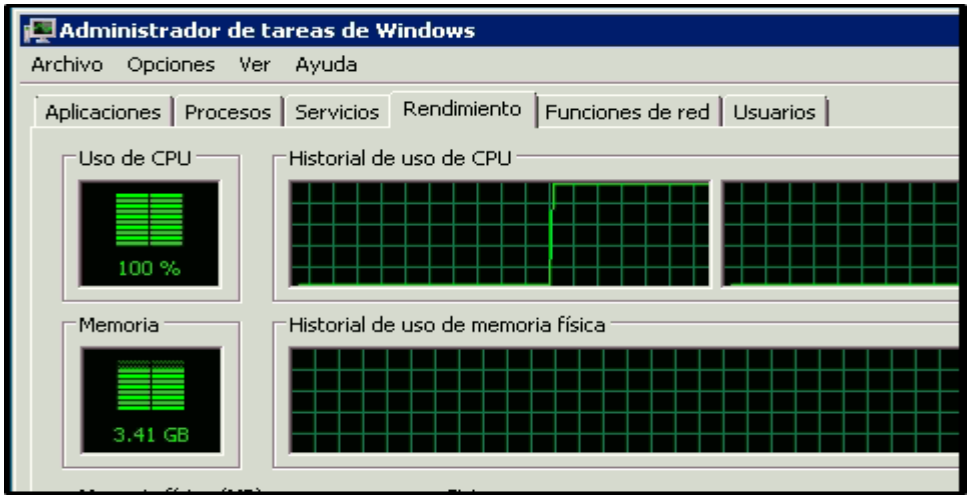

Figura 3. Sobrecarga del CPU

***Fuente**: Oré, C. (2019)*

Uno de los problemas que afecta directamente a los clientes dentro de la organización es acceder a su información que se encuentra en la carpeta compartida del File Server, no hay espacio suficiente para salvaguardar su información, y a su vez el respaldo de backup que se genera cada cierto tiempo de manera automática dentro de los servidores.

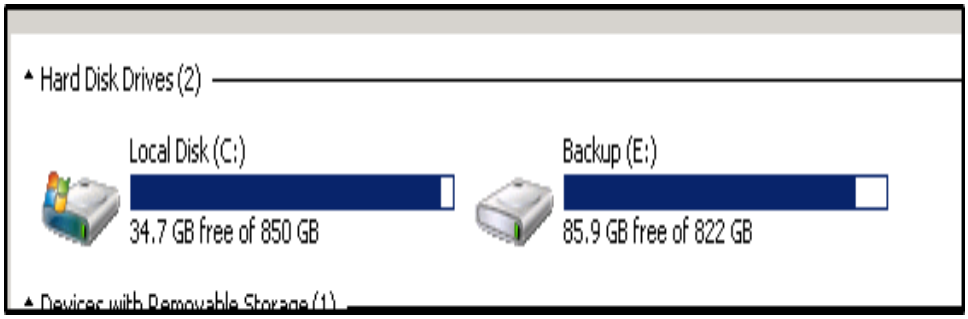

Figura 4. File server

***Fuente**: Oré, C. (2019)*

Problemas con la recepción y salida de correos, encolamiento de correos SMTP relay.

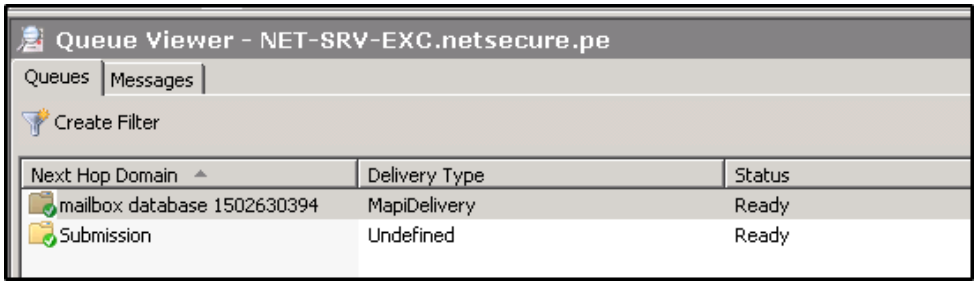

Figura 5. SMTP relay

***Fuente**: Oré, C. (2019)*

Problemas con la disponibilidad para acceder al sistema de Gestión de tickets, generando una disconformidad por parte del cliente y de los trabajadores de la organización.

Figura 6. Gestión de tickets

***Fuente**: Oré, C. (2019)*

Una red lenta o de baja performance es un verdadero problema para la organización ya que genera pérdida de productividad, identificar la raíz del problema a tiempo es muy complicado para el ingeniero a cargo. Existen varias causas para que se genere lentitud en la red, entre las más destacadas son:

- Placas de red defectuosas
- Fallas en switches o router
- Conflictos de IP
- Exceso de aplicaciones que operan sobre la red

También se han presentado en el pasado algunos eventos que afectan directamente la disponibilidad de los servicios en la sede Villa el Salvador, la caída de uno de los equipos Firewall perdiendo gestión de todos los servicios, habiendo una demora en el desplazamiento para llegar al Data center. Por lo que, con la finalidad de poder identificar las causas de la problemática central, se utilizara la técnica del árbol de problemas, a través de la cual se ha elaborado los siguientes gráficos:

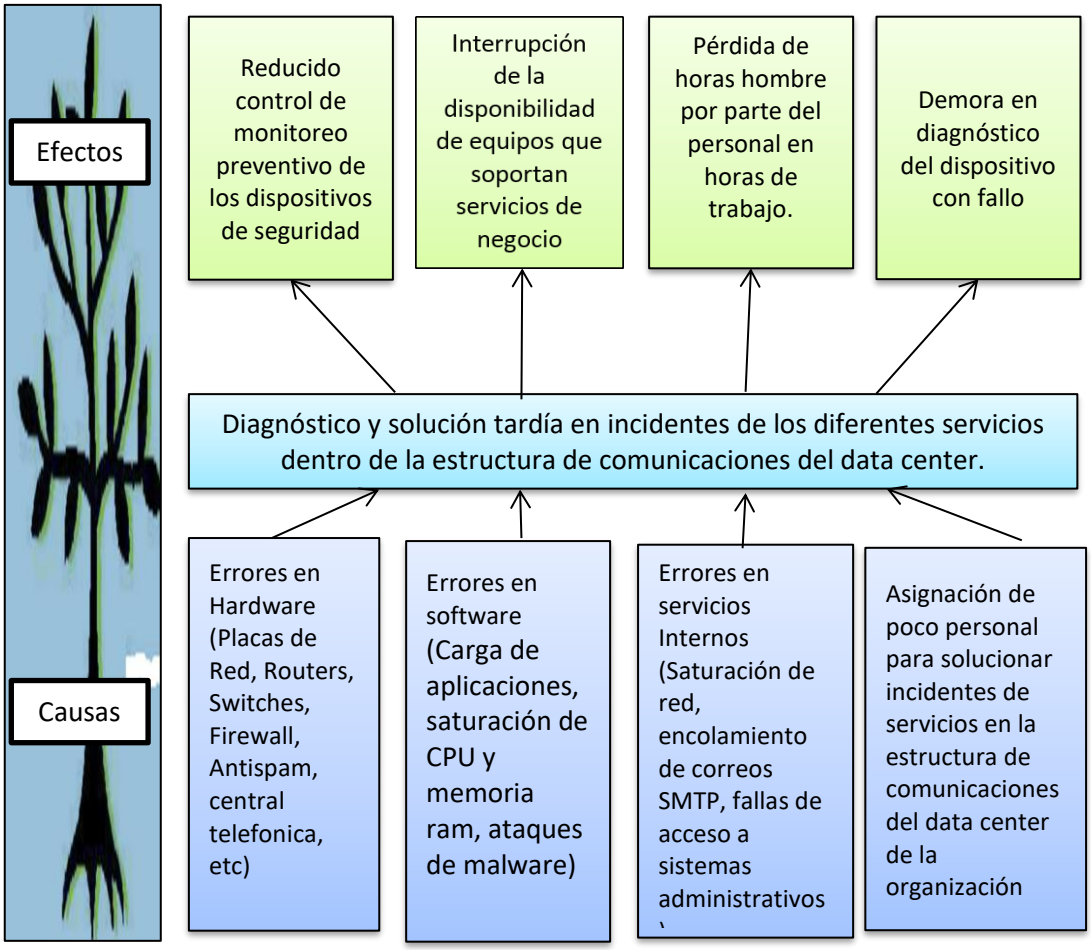

Figura 7. Árbol del problema

***Fuente**: Oré, C. (2019)*

Tabla 1. Árbol del problema

Árbol de Problemas	
Definición del Problema: Diagnóstico y solución tardía en incidentes de los diferentes servicios dentro de la estructura de comunicaciones de la data center de la organización.	
Causas:	Efectos:
• Errores en hardware (Placas de red, routers, Switches, Firewalls, Antispam, Anti DDOS, etc). • Errores en software (Carga de aplicaciones, saturación de CPU y memoria ram, ataques de malware) • Errores en servicios Internos (Saturación de red, encolamiento de correos SMTP, fallas de acceso a sistemas administrativos) • Asignación de poco personal para solucionar incidentes de servicios en la estructura de comunicaciones de la data center de la organización	• Reducido control de monitoreo preventivo de los dispositivos de seguridad • Interrupción de la disponibilidad de equipos que soportan servicios de negocio • Pérdida de horas hombre por parte del personal en horas de trabajo. • Demora en diagnóstico del dispositivo con fallo

***Fuente**: Oré, C. (2019)*

En el cuadro (tabla. 1) se muestra las cuatro causas más importantes que genera un problema central y que esta a su vez tiene efectos negativos para la empresa. Como primera causa se tienen los errores en servicios internos, originados por saturación de red, encolamiento o fallas de acceso a sistemas administrativos.

Entre los efectos más importantes mostrados (fig. 7) se observa la perdida de horas hombre por parte del personal en horas de trabajo, lo que comúnmente se denomina tiempos muertos, que mucho depende de la demora en el diagnóstico del dispositivo para dar con la solución del mismo.

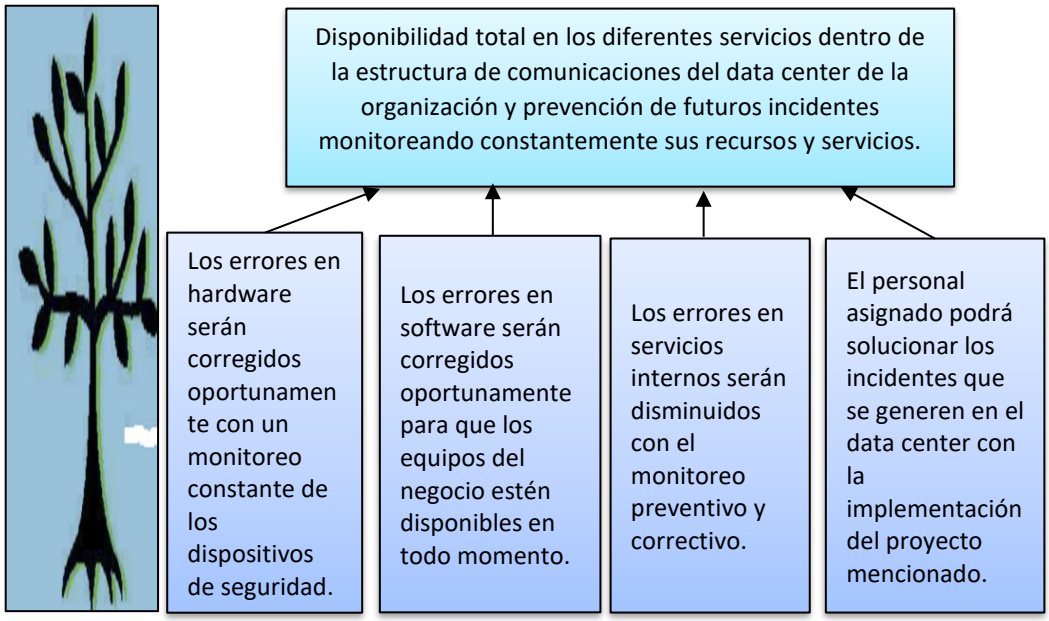

Figura 8. Árbol de los objetivos

***Fuente**: Oré, C. (2019)*

Se agrega el árbol de objetivos para reforzar la solución al problema descrito (fig. 8).

- Aumentar el control del monitoreo preventivo en los dispositivos de seguridad, ya que los controles de monitoreo en un zona específica acceden monitorear labores y tomar medidas para hacer una corrección inmediata o preventivas para evitar eventos expuestos en el futuro.
- Mantener disponible en todo momento, los equipos que soportan los servicios del negocio corrigiendo oportunamente los equipos, estos servicios de red y datos seguros brindan a la empresa una red segura y general con soluciones de equipos siendo respaldadas y ayudando a mantener su conectividad e incorporar los equipos más actuales, tantos equipos de redes y voz, para que se obtenga una pronta solución que ayude a la empresa.

- Reducción en pérdida de horas hombre por parte del personal disminuyendo los tiempos muertos por falla en equipos, esto tiene como finalidad resolver en un tiempo prudencial y con la mayor eficiencia aquellos objetivos que se tengan planteados. En tal sentido se indica que los mayores problemas y situaciones de la gestión del tiempo son la dispersión y la dilación.
- Reducir el tiempo de diagnóstico en dispositivos con fallo con monitoreos preventivos y correctivos, esto consiste en un tipo de mantenimiento que permite tomar acciones para prevenir el deterioro del sistema de monitoreo; ya que, no es solamente una acción de limpieza, sino una dinámica de métodos y que ejercitándolas brindan grandes satisfacciones al momento de la revisión y solución de fallos con los monitores.

1.3.2 Proyecto Propuesto

Es importante comprender que, el esquema de monitorización planteado intenta informar la correcta actuación de la red, los servidores y servicios, el cual se halla orientado a desarrollarse en una de las empresas más acreditadas en el ámbito de la tecnología de la informática Netsecure Perú Informática.

Para ello, es significativo reconocer el estado de los sistemas que se manipulan dentro de la organización que consientan garantizar la correcta maniobra de los mismos y no perder tiempo y dinero, es necesario que estos sistemas se conserven prestando el servicio el mayor tiempo posible y sin obstáculos, si existiera una falla o situaciones inusuales, como podría ser el caso cuando un servidor se quede sin suministro de energía eléctrica, exceso de sobrecarga de CPU, Memoria y Capacidad, condiciones ambientales de temperatura mayor a los 27° C, reinicio automático de servicios, incremento de la conexión a Internet debido a un mayor uso del ancho de banda la cual nos podría indicar un potencial ataque.

De esta manera, tendrá que notificar al Ingeniero a cargo para que pueda actuar de manera proactiva a fin de evitar una negativa de servicios o desgaste de información. Debido a esta situación el presente proyecto planea la implementar un sistema de monitoreo utilizando el protocolo Simple Network Management Protocol (SNMP), con ayuda de la herramienta PRTG Network Monitor la cual nos va permitir ayudar a monitorear de manera eficiente, y ser capaz de resolver incidencias de forma rápida y, más que eso, ser capaz de anticiparse en la prevención de situaciones críticas de extrema relevancia, con el fin de certificar la continuidad de la operación de los recursos de TI sin afectar los procesos de negocio.

El seguimiento de algunos indicadores puede ayudar mucho en una acción proactiva para el equipo de TI, ayuda a descubrir los problemas y evita antes de que estas sucedan, minutos de interrupción puede costar muy caro a la organización.

1.4. Objetivos del Proyecto

1.4.1 Objetivo General del Proyecto

Implementar un sistema de monitoreo de red, para la observación del comportamiento de la infraestructura de comunicación de la empresa Netsecure Perú, avalando la detección rápida de sucesos y el aseguramiento de la continuidad de los servicios de la data center.

1. Analizar las generalidades de la empresa con la finalidad de obtención de un mejor servicio.
2. Desarrollar un sistema de monitoreo de red, para la observación del comportamiento de la infraestructura de comunicaciones de la empresa Netsecure Perú, garantizando la detección inmediata de incidentes y el aseguramiento de la continuidad de los servicios de la data center.

3. Determinar la factibilidad económica y financiera de la implementación de un sistema de monitoreo de red, para la observación del comportamiento de la infraestructura de comunicaciones de la empresa Netsecure Perú, garantizando la detección inmediata de incidentes y el aseguramiento de la continuidad de los servicios de la data center.

.

CAPITULO 2: FUNDAMENTO TEÓRICO

2.1. Antecedentes

Actualmente la humanidad se mueve a una rapidez sorprendente. Todos los días aparecen nuevos productos en el comercio que sustituyen a los hoy existentes. La actualidad, lo novedoso y las producciones en general tienen, en su totalidad, un período de vida breve. Los mercados se tornan muy competitivos y para lograr insertarse en ellos es necesaria la inmutable transformación. Los cambios tecnológicos ocurren tan vertiginosos que se ha acabado de asimilar la tecnología actual y de inmediato aparece otra. La indagación de la competencia de las producciones es una labor de primera disposición para la directiva de la empresa. El progreso del conocimiento innovadora constituye un aspecto esencial para las áreas de infraestructura, así a partir del propósito de una habilidad de ciencia e innovación tecnológica se debe lograr un adecuado nivel de gestión de conjunto de técnicas que posibilite la ventaja e incorporación de nuevos conocimientos científico-tecnológicos a la actividad productiva de la organización Netsecure Perú, con el objetivo de conservar e acrecentar sus niveles de competencia y eficiencia con los esquemas internacionales de calidad.

Se ha sentido una fuerte tendencia a optimizar los procesos y mejorar la productividad a través de la tecnología lo cual se convierte en un reto para las áreas de sistemas e infraestructura en cuanto a la adquisición de hardware, software y equipos de TI. Lo cual llega a ser un nuevo reto a controlar y medir para tomar acciones contra eventos que puedan ocurrir dentro de los centros de datos, donde lo tecnológico es uno de los aspectos más importantes para que una compañía logre el éxito (León, 2008, p. 34).

2.1.1. Caso de éxito

Caso de éxito – Beliveo (México)

Beliveo es una empresa de Outsourcing dedicada a dar soporte vía Call Center a empresas de todo tipo. Fundada en 2012 se especializa en ofrecer servicio de exportación a clientes de EU. Al día de hoy cuenta con

más de 1,100 colaboradores ofreciendo servicio a clientes incluidos en la lista de Fortune 100.

Beliveo tiene clientes de sectores medios de comunicación, entretenimiento y televisión de paga. Con oficinas en Guadalajara y Monterrey, continúa con su prometedor crecimiento dentro del mercado de los Centros de Llamadas exitosos en el mundo (Paessler, 2014).

Reto

Poder evitar contingencias derivadas de fallas nocturnas en equipos de la infraestructura, el monitorear en tiempo real los 500 terminales, 30 aplicaciones, y casi 100 dispositivos como 12 ruteadores, 24 switches, 20 servidores y firewalls, además de utilizar una sonda remota para la monitorización de redes externas en EU y ser alertados a tiempo a fin de poder tomar una acción correctiva (Paessler, 2014).

Solución

La solución PRTG ha traído a Beliveo grandes beneficios como:

- Resolver problemas en cuanto a la saturación de ancho de banda, detectando la fuente de los problemas con datos de Netflow.
- Ayuda total en contar con las ventajas de tener un producto que apoya en la proactividad de acciones que evitan tiempo de inactividad.
- Con el sistema descubrieron que no es necesario tener personal 24x7 de monitoreo, ya que fue resuelto con las alertas a dispositivos móviles en forma de notificaciones Push.
- Ahorro de tiempo del 80% en fallas durante la noche.
- Evitar hasta 70% menos en alarmas o incidencias (Paessler, 2014).

Caso de éxito – GESAC (Italia)

Gesac - Airport Services Management Campani - es una empresa de gestión del Aeropuerto Internacional de Nápoles, una entidad de referencia para la funcionalidad y seguridad de las infraestructuras de todo el sistema aeroportuario. La empresa, que hoy cuenta con alrededor de 400 empleados, se estableció en 1980, con una mayoría pública, por iniciativa del Municipio de Nápoles, la Provincia de Nápoles y Alitalia (CEPAL, 2011).

Para convertirse en la principal puerta de entrada del sur de Italia y facilitar la experiencia de los pasajeros, Gesac se reconoce en tres valores fundamentales: innovación, mejorar la calidad del servicio y la experiencia del pasajero; la naturaleza esencial de los procesos, basada en la simplicidad y la fluidez para resultados concretos y mensurables; la responsabilidad por los comportamientos y los resultados para estimular el espíritu de iniciativa (CEPAL, 2011).

Reto

Asumiendo un rol de suma importancia para la actividad de los sistemas operativos de los aeropuertos, la infraestructura de TI del aeropuerto de Nápoles es demasiada compleja. Gesac es garante de la gestión, conexión y observación técnico-operativa de más de 1000 dispositivos distribuidos en servidores y PCs que gobiernan los sistemas de seguridad críticos. Poder contar con una solución de monitoreo, diagnóstico y administración de infraestructuras de red de última generación es, por lo tanto, crucial para una realidad tan compleja como es el aeropuerto (CEPAL, 2011).

De hecho, existen muchos requisitos, en primer lugar, la posibilidad de realizar análisis oportunos para garantizar la continuidad de las infraestructuras, para interceptar rápidamente cualquier problema crítico que, si no se resuelve, podría provocar el colapso de los sistemas, lo cual no es lo deseado.

Solución

La solución de software trajo beneficios significativos en términos de consolidación de aplicaciones, reducción de inversiones en infraestructura, mejor continuidad de servicio, mayor eficiencia de software, que en cuestión de meses resultó en un aumento general en la eficiencia del hardware y una consiguiente reducción del perímetro técnico monitoreado. PRTG Network Monitor proporciona soporte concreto para informar los primeros problemas críticos a través de umbrales de advertencia predeterminados que permiten intervenciones rápidas de gestión y resolución de amenazas potenciales Gesac (CEPAL, 2011).

Por lo que se ha identificado en PRTG Network Monitor la mejor tecnología en términos de calidad, eficiencia y confiabilidad, pudiendo contar con la disponibilidad continua de actualizaciones y un servicio de soporte de alto nivel, facilidad de implementación e integración con sistemas externos y la extrema simplicidad de uso (CEPAL, 2011).

2.1.2. Datacenter

Según COMPLETHOST LTD, (2014) un centro de procesamiento de datos (CPD) es la localización física donde se reúnen servidores, equipo de almacenamiento y procesamiento de sistemas y datos de activos de red, como switches, enrutadores y otros. Por ello, es calificado el sistema nervioso de las empresas. Dentro de las particularidades que posee un data center y en concordancia a explicación de los expertos en la materia están:

Energía garantizada

Uno de los factores más importantes para mantener la buena marcha del Data Center está considerablemente relacionado con la energía eléctrica que se encarga de alimentarlo. Sin la energía eléctrica íntegra, este tipo de estructura no marcharía de forma correcta y provocaría pérdidas a la empresa.

Por ende, no basta con estar conectado a la energía eléctrica tradicional, sino que es preciso contar con equipos específicos la cual sea capaz de contribuir con energía eléctrica para optimar la buena actividad, un método de emergencia que se active en caso de que no haya luz, como los generadores eléctricos UPS y Grupo electrógenos.
Son parte primordial para afirmar el servicio en caso de un corte de energía.

Conexión a Internet

Los datos están conectados a internet a través de conexiones Gigabit Ethernet redundantes, lo que significa, en caso de falla de una línea, el servicio seguirá marchando sin problemas.

Seguridad

Por la cantidad de información importante que es bastante, se guardan en los servidores albergados en el data center, la seguridad es un tema esencial para evitar cualquier tipo de robo de información u otros tipos de situaciones esto podría resultar desastroso para la organización. Servicios de video vigilancia y con la presencia de un administrador de red las 24 horas del día son ciertas medidas que todo centro de datos debe efectuar para así certificar la seguridad de la información de los clientes.

Climatización:

Es necesario mantener un centro de datos en una temperatura promedio de 15 a 25 grados para evitar humedad en los equipos eléctricos. Es por esta razón que los centros de datos utilizan sistemas de aire acondicionado de precisión que mantienen la temperatura, evitando el sobrecalentamiento de los servidores y otros dispositivos que se encuentran encendidos las 24 horas de los 365 días (Torres, 2017).

2.1.3. Gestión de red

La gestión de red implica el despliegue, la integración y la coordinación de todo el hardware, software y elementos humanos para monitorear, probar, sondear, configurar, analizar, evaluar y controlar los recursos de la red, con la finalidad de cumplir con el rendimiento operativo, en tiempo real y con calidad de servicio (QoS) (IJEAT, 2015). Cabe destacar que un sistema de gestión de red dispone de tres tipos principales de recursos:

- **Métodos de gestión:** Definen las pautas de comportamiento de los demás componentes del centro de gestión de red ante determinadas circunstancias.
- **Recursos humanos:** Personal encargado del correcto funcionamiento del centro de gestión de red.
- **Herramientas de apoyo:** Herramientas que facilitan las tareas de gestión a los operadores humanos y posibilitan minimizar el número de éstos.

2.1.4. Modelo OSI

El funcionamiento de las redes informáticas está basado en varios estándares y se encuentran definidos en el modelo de referencia OSI la cual es una normativa formada por siete capas que define las diferentes fases por las que deben pasar los datos para viajar de un dispositivo a otro sobre una red de comunicaciones (Calderón, 2018, p. 13).

De allí que, según el autor antes mencionado cada capa del modelo de referencia OSI se describe de la siguiente manera:

- **Capa Física:** La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales. Las características tales como niveles de voltaje, temporización de cambios de voltaje,

velocidad de datos físicos, distancias de transmisión máximas, conectores físicos.

- **Capa de enlace de datos:** Proporciona tránsito de datos confiable a través de un enlace físico. Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico (Comparado con el lógico), la topología de red, el acceso a la red, la notificación de errores, entrega ordenada de tramas y control de flujo.
- **Capa de Red:** Es una capa compleja donde se lleva a cabo el direccionamiento lógico que tiene carácter jerárquico, selecciona la mejor ruta hacia el destino mediante el uso de tablas de enrutamiento a través del uso de protocolos de enrutamiento o por direccionamiento estático. La capa de red debe gestionar la congestión de red, que es el fenómeno que se produce cuando una saturación de un nodo tira abajo toda la red. Los protocolos de capa de red: IP, IPX, RIP, IGRP, Apple Talk.
- **Capa de Transporte:** Su función básica es aceptar los datos enviados por las capas superiores, dividirlos en pequeñas unidades si es necesario, y pasarlos a la capa de red. En el caso del modelo OSI, también se asegura que lleguen correctamente al otro lado de la comunicación.
- En esta capa se proveen servicios de conexión para la capa de sesión que serán utilizados finalmente por los usuarios de la red al enviar y recibir paquetes.
- **Capa de Sesión:** Esta capa ofrece varios servicios que son cruciales para la comunicación, es la responsable de establecer, administrar y finalizar las sesiones entre dos hosts que se están comunicando. La comunicación en esta capa consiste en peticiones de servicios y respuestas entre aplicaciones ubicadas en diferentes dispositivos.

- **Capa de Presentación:** La capa de presentación garantiza que la información que envía la capa de aplicación de un sistema pueda ser leída por la capa de aplicación de otro. De ser necesario, la capa de presentación traduce entre varios formatos de datos utilizando un formato común
- **Capa de Aplicación:** Dos ordenadores se intercomunican a través de procesos, correspondiente a unas determinadas aplicaciones. El intercambio de información entre dos procesos se efectúa por medio de algún protocolo de la capa de aplicación. Mencionaremos algunos protocolos de la capa de aplicación son TELNET, FTP, SMTP, POP3, DNS, RTP, HTTPS. (ISO, s/f)

En concordancia con ello, se presenta una breve descripción de cada capa del modelo de referencia OSI tal como aparece en la figura:

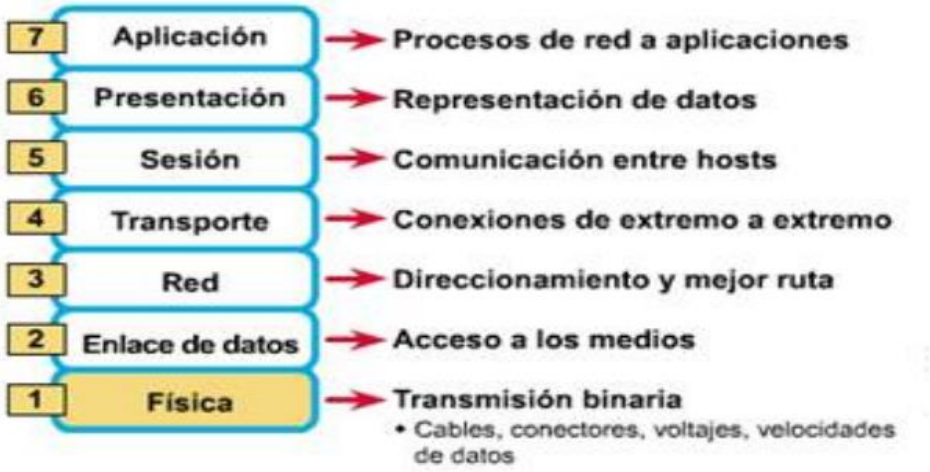

Figura 9. Capas de modelo OSI

Fuente: Cisco (2017)

2.1.5. Administrador de red

Conocido también como administrador de sistemas, es la persona encargada de supervisar y controlar el hardware y software de una red interna. Este es el responsable de mantener la red informática actualizada y en continuo funcionamiento, en caso de que haya fallas en el sistema,

poder solucionarlos de la forma más rápida y eficaz posible (COMPLETHOST LTD, 2014). La administración de red puede ser difícil por tres razones:

- La mayoría de las redes locales son heterogéneas, quiere decir que son de diferentes fabricantes.
- Se mezclan diversas señales como voz, datos, imágenes y gráficas.
- Los dispositivos de red en las redes locales para cada una de estas oficinas se encuentran en puntos alejados geográficamente.

Es importante trabajar con un sistema de monitoreo que permita centralizar los dispositivos de red desde un solo punto geográfico. Este proyecto describe un sistema de gestión de monitoreo centralizado para la empresa Netsecure Perú, uno de los elementos más importantes para que un administrador de red desempeñe un buen funcionamiento en la gestión de la red, es utilizando el protocolo llamado Simple Network Management Protocol SNMP.

2.1.6. SNMP

Según COMPLETHOST LTD, (2014), el Protocolo Simple de Administración de Red (Simple Network Management Protocol) es un protocolo de internet para el manejo de dispositivos dentro de redes IP y pertenece a la capa de aplicación. Switches, routers y servidores son ejemplos de equipos que contienen objetos gestionables. Estos objetos son información de hardware, así como los parámetros directamente relacionados con el comportamiento del equipo en cuestión. Es un protocolo de gestión de red muy utilizado ya que permite obtener información de dispositivos de la red, memoria libre, uso de CPU, detección de errores, establecer alarmas, estado de funcionamientos, etc.

2.1.6.1. Componentes SNMP

Una red administrada a través de SNMP consta de cuatro componentes clave:

- **Dispositivos administrados:**

  Es un dispositivo que contiene un agente SNMP y reside en una red administrada. Estos recogen y almacenan información de administración, la cual es puesta a disposición de los NMS's usando SNMP.

- **Agentes:**

  Es un módulo de software que traduce la información del dispositivo en un formato compatible con SNMP para que la información del dispositivo esté disponible para monitorear con SNMP. El agente recibe las solicitudes por el puerto 161 UDP, facilitando el acceso a la información en los equipos administrados.

- **Sistemas de gestión de red (NMS):**

  Ejecuta aplicaciones de monitoreo, proporcionan la mayor parte de los recursos de procesamiento y memoria necesarios para la administración de la red, uno o más NMS deben existir en cualquier red administrada.

- **Base de información de administración (MIB):**

  Es la base que contiene la información del estado del sistema, las estadísticas de rendimiento y los parámetros de configuración. Se puede acceder al MIB mediante un protocolo de administración de red como es el caso de SNMP. Toda la información se encuentra organizada jerárquicamente.

2.1.6.2. Mensaje SNMP

SNMP Define ocho tipos de mensajes de intercambio entre gestor y agente que se denominan PDUs (Unidad de datos de Protocolo):

- **Get request:** Solicita uno o más valores de un objeto. El nodo administrador transmite y el agente que contesta recibe.
- **Get Bulk Request (en Snmp v2):** Solicita un conjunto amplio de atributos en vez de solicitar uno a uno. El nodo administrador transmite y el agente recibe.
- **Get next request:** Solicita el atributo siguiente de un objeto. El nodo administrador transmite y el agente recibe.
- **Set request:** Actualiza uno o varios atributos de un objeto. El nodo administrador transmite y el agente recibe.
- **Set Next Request:** El siguiente atributo de un objeto lo actualiza. El nodo administrador transmite y el agente recibe.
- **Get Response:** Los atributos solicitados los devuelve. El agente transmite y el nodo administrador recibe.
- **Trap:** Permite a un agente notificar ciertos eventos significativos como las fallas, pérdida de la comunicación, caída de un servicio, voltajes fuera de rango, etc. El agente transmite y el nodo administrador recibe.
- **Inform Request (en Snmp v2):** Describe la base local MIB para intercambiar información entre los nodos de administración. El nodo administrador transmite y recibe.

2.1.6.3. Versiones SNMP

Las versiones de SNMP más utilizadas son:

- **SNMP v1:** Esta es la versión más antigua y básica de SNMP. Su seguridad es limitada porque solo usa una contraseña simple (cadena de comunidad) y envía datos en texto sin cifrar, esta versión no se distribuye en dispositivos actuales.
- **SNMP v2C:** Tiene características similares en común con la versión 1, utiliza el mismo modelo administrativo que la primera versión del protocolo SNMP, y no incluye mecanismos de seguridad. Las únicas

mejoras introducidas en la versión 2 consisten en una mayor flexibilidad de los mecanismos de control de acceso, ya que se permite la definición de políticas de acceso consistentes en asociar un nombre de comunidad con un perfil de comunidad formado por una vista MIB y unos derechos de acceso a dicha vista (read-only o read-write).

- **SNMP V3:** Éste agrega soporte para una autenticación más segura y comunicación privada entre entidades administradas. Es un protocolo de manejo de red interoperable, que proporciona seguridad de acceso a los dispositivos por medio de una combinación de autenticación y cifrado de paquetes que trafican por la red.

2.1.7. Conceptos Relevantes a la aplicación

2.1.7.1. Software PRTG Network Monitor

PRTG Network Monitor es una poderosa herramienta de monitoreo, basada en la plataforma operativa Windows, adecuada para redes de pequeño, mediano y grande, capaz de monitorear LANs, WANs, WLAN y VPNs en lo que se refiere a la disponibilidad de la red y uso de banda, así como varios otros parámetros, tales como calidad de servicio, carga de memoria, uso de CPU, sistemas Linux, sistemas Windows, routers, switches, servidores de correo, servidores de archivos, y mucho más.

Permite a los administradores de sistemas y redes obtener información como: lecturas de informes y gráficos de datos generados en tiempo real y periódicos, previsión de las tendencias de uso con el objetivo de optimizar la eficiencia del sistema de red y evitar posibles problemas, entre otras.

Para recopilar los datos y hacer el monitoreo, el PRTG se utiliza de muchos protocolos de gestión de redes conocidos, entre ellos se destacan: Protocolo simple de administración de redes (SNMP), Instrumento de administración de Windows (WMI), paquete de sniffer, Cisco NetFlow (así

como sFlow y jFlow) y muchos otros. Todos los datos recogidos por estos protocolos se almacenan en una base de datos interna proporcionando una visión a largo plazo sobre el estado general y sobre el uso de la red. Siempre que se detecta una posible amenaza al rendimiento, el PRTG emite una alerta que puede llegar al administrador por correo electrónico, mensaje de texto (SMS), informe de datos en la pantalla de un ordenador o un teléfono móvil. Hay que tener claro los siguientes términos:

Jerarquía de objetos

En una configuración de monitoreo del PRTG, los objetos están todos dispuestos en una jerarquía de árbol, permitiendo una navegación más organizada, brindando al administrador de red la posibilidad de separar los objetos en grupos y monitorear dispositivos y servicios similares (COMPLETHOST LTD, 2014).

Figura 10. Modelo de la Jerarquía de objetos de PRTG

Fuente: Cisco (2017)

Grupo "Root"

Esta es la instancia superior en la jerarquía de objetos del PRTG que contiene todos los demás objetos en su configuración. Usando el mecanismo de herencia, se recomienda ajustar la configuración predeterminada en el grupo de raíz para que todos los demás objetos puedan heredarlos. Esto facilitas configuraciones posteriores (COMPLETHOST LTD, 2014).

Sonda

Esta es la base de la cual funciona la monitorización, todos los objetos configurados bajo una sonda son monitorizados por esta sonda. Cada instalación núcleo de PRTG automáticamente instala un servicio de sonda local (COMPLETHOST LTD, 2014).

Grupo

En cada Sonda pueden existir uno o más grupos, cuya finalidad principal es organizar de forma lógica objetos similares (COMPLETHOST LTD, 2014).

Aparato

Para el PRTG, cada dispositivo representa un dispositivo real de la red, que se puede controlar. En cada Sonda o Grupo, debe agregar los dispositivos que desea supervisar (COMPLETHOST LTD, 2014).

Sensor

Bajo cada aparato puede generar un número de sensores, cada sensor monitoriza un aspecto del aparato. Esto puede ser, por ejemplo: un servicio de red, como Ping, HTTP, FTP, SMTP, POP3, DNS y muchos otros (COMPLETHOST LTD, 2014).

Canal

Cada sensor tiene un número de canales por medio de los cuales procesa y visualiza los diferentes tramos de datos, los canales disponibles dependen del tipo de sensor. Un sensor, por ejemplo, puede contener los siguientes canales: Tiempo de falla de un aparato, tráfico de entrada y salida de un aparato (Ancho de banda), tráfico de correo, carga de procesador entre otros.

2.1.7.2. Importancia

El sistema de monitorización PRTG se fue impulsando durante varios meses, debido a que la eficiencia de la monitorización, la detección oportuna de fallas, las alertas y los reportes son actividades de gran relevancia para brindar un buen servicio a los usuarios. De esto se deriva la importancia de contar con un sistema de monitoreo capaz de notificar las fallas en la red y de mostrar su comportamiento mediante el análisis y recolección de tráfico Es por ello que la empresa Netsecure Perú logró comprar un licenciamiento más amplio y con ello se logró tener una monitorización más completa de toda la infraestructura.

Un sistema de monitorización se resume en productividad, y es uno de los puntos críticos que todo departamento de informática debe tener: permite el desempeño y el orden de todos los recursos tecnológicos de la organización, tales como el ancho de banda, tiempos, acceso a servidores, velocidad, uso de memoria RAM, uso de CPU, direcciones IP, actualizaciones de sistema, velocidad de ventiladores y voltajes, controles, pérdida de información, pérdida de emails, control de malware y más.

2.1.7.3. Características

Este software PRTG es de gran utilidad a continuación se detallan algunas de las cualidades de esta herramienta:

- **Monitorización de Trafico, uso, rendimiento y disponibilidad:** Mediante las estadísticas que muestran los totales (disponibilidad, ancho de banda / tráfico, carga CPU, alertas) nos podemos informar rápidamente sobre el estado actual de toda la red. Los estados se pueden mostrar para todos los sensores, y por grupo. De este modo, podemos tener una vista general de toda la red y de cada dispositivo.
- **Clasificar el uso de la banda ancha según IP, protocolo o conexión:** Para saber qué aplicaciones o direcciones IP están causando el tráfico en nuestras redes podemos utilizar packet sniffing (PRTG analiza cada paquete de datos que pasa por la red) o el monitoreo basado en NetFlow/jFlow/sFlow. Usando cualquiera de estas tecnologías, PRTG puede analizar el uso de la banda ancha y atribuirlo a protocolos u ordenadores en la red.
- **Gestión jerárquica de equipos y sensores:** En PRTG Network Monitor los "sensores" se encargan de la monitorización. Los sensores se organizan en forma de árbol para crear una lista que podemos navegar con facilidad y que nos permite agrupar equipos, sitios o servicios similares. Los usuarios podemos crear grupos anidados: Cada grupo puede contener varios equipos, y cada equipo varios sensores.
- **Alarmas, advertencias y alertas por estados inusuales:** Las alarmas (rojas) son sensores no disponibles (p.ej. debido a un fallo del software o hardware) o que traspasan un valor definido (p.ej. espacio libre de disco duro por debajo del 10%). Las advertencias (amarillas) son causados por servicios lentos (p.ej. una página web que carga demasiado lenta) o por recursos que están a punto de agotarse (p.ej. baja memoria RAM o alta carga de CPU), PRTG marca sensores con un estado inusual (naranja) si los valores actuales discrepan mucho de los valores históricos (calculado a través de un análisis estadístico).

Listas Top 10.

Las listas "Top 10" son según Chicaiza, (2014) unas herramientas potentes para conseguir una vista rápida de todos los sistemas en la red, y para encontrar posibles problemas. Las listas Top 10 están disponibles para:

- Disponibilidad más alta y más baja.
- Los tiempos de PING más rápidos y más lentos.
- Uso de la banda ancha más alto y más bajo.
- Páginas webs más rápidas y más lentas.
- Carga CPU más alta y más baja.
- Más y menos espacio de disco duro libre.

Informes exhaustivos

Los informes se usan para analizar los resultados del monitoreo durante un tiempo específico, como por ejemplo un día, un mes o un año. PRTG incluye una potente función de informes para generar informes tanto en el momento o programados con anterioridad (p.ej. una vez al día). Se pueden crear informes para uno o varios sensores. El contenido y el diseño dependen de la plantilla de informes seleccionada y se aplican a todos los sensores en el informe (Chicaiza, 2014).

Crear mapas con datos de monitoreo en directo

Los mapas combinan el estado de sensores, gráficos y tablas. Podemos crear tantos mapas que queremos, y personalizar el diseño y los fondos con mapas de la red, mapas geográficos, etc. Crear el diseño es fácil utilizando drag&drop desde la misma interfaz web de PRTG. Los mapas de PRTG se basan en un concepto innovador que nos permite de crear páginas webs con información de estado del momento en un diseño personalizado (Chicaiza, 2014). Esto nos abre incontables posibilidades para la implementación de mapas. Por ejemplo, se puede utilizar esta función para:

- Diseñar mapas de redes sobreponiendo iconos de estado para cada equipo en el mapa.
- Crear paneles de control que podemos mostrar en las pantallas de nuestro centro de datos.
- Crear una vista rápida de la red para publicación en la Intranet para que la dirección de la empresa y otros empleados puedan informarse.
- Crear vistas personalizadas de los sensores más importantes de nuestra monitorización de red.
- Crear listas Top 10 para los sensores de un grupo o equipo determinado.

PRTG es adecuado para redes con 100 o 10.000 sensores

PRTG Network Monitor es apto para redes de todos los tamaños. Se puede utilizar en redes pequeñas con pocos equipos (por ejemplo, utilizando la versión gratuita, que permite monitorear hasta 10 sensores), o bien se puede integrar en redes grandes con 10.000 sensores o más (del momento, el software puede monitorizar hasta 20.000 sensores en una sola instalación), (PRTG, 2018).

2.1.7.4. Versatilidad

La versatilidad de PRTG lo hace la herramienta perfecta para el monitoreo de redes de todos los tamaños. En este punto cabe describir lo siguiente:

Interfaces de usuario

Interfaz web con toda la funcionalidad: tecnología web moderna, basada en AJAX.

- Sólo HTML, interfaz web minimalista (funcionalidad limitada) para navegadores antiguos y dispositivos móviles (funciona con IE6/7/8, iPhone, Android, Blackberry).

- Enterprise Console: aplicación Windows, especialmente diseñada para grandes instalaciones. Se pueden ver los datos de monitoreo de varias instalaciones de PRTG en una aplicación.
- Apps para iOS (iPhone/iPad) y Android smartphones: Siga el estado de la red, aunque esté viajando (hay que descargarlo/comprarlo por separado).
- Todas las interfaces permiten el acceso local y remoto protegido por SSL y pueden ser utilizados simultáneamente.

Tipos de monitoreo

- Más de 150 tipos de sensores cubren todos los aspectos de monitoreo de la red que se requiera monitorear.
- Existe la supervisión del tiempo, en cuanto al funcionamiento y periodos de inactividad (uptime / downtime).
- Se puede realizar una monitorización de ancho de banda utilizando SNMP, WMI, NetFlow, sFlow, jFlow, packet sniffing.

Existe una gran cantidad de monitoreos a continuación se detalla una lista de los tipos que se pueden realizar:

Monitoreo de aplicaciones

- Monitoreo web.
- Monitoreo de servidores virtuales.
- Monitoreo de SLA (acuerdo de nivel de servicio).
- Monitorización QoS (Calidad de servicio, por ejemplo, para monitorizar VoIP).
- Monitoreo ambiental.
- Monitorización de LAN, WAN, VPN, y sitios distribuidos.
- Registro extenso de eventos (Extensive event logging).
- Soporte de IPv6.

- Monitoreo sin agentes (agentes opcionales (remote probes) permiten una monitorización incluso más detallada).
- Sistema de alertas.
- Tecnologías de notificación: envío de mensajes de correo electrónico, SMS/pager, syslog y SNMP Trap, HTTP request, event log entry, reproducir archivos de audio, Amazon SNS y cualquier tecnología externa que pueda ser ejecutado por un fichero EXE o batch.
- Alertas de estado (up, down, aviso).
- Alertas de límites (valor por debajo / encima de x).
- Umbrales (por debajo / encima de x durante z minutos).
- Alertas con múltiples condiciones (tanto x como z están inactivos).
- Alertas de escalación (notificaciones adicionales cada x minutos durante el tiempo de inactividad).
- Dependencias (para evitar una ola de alertas).
- Alertas reconocidas (no se mandan más notificaciones para esta alarma).
- Programación de alertas (pare evitar alertas de baja prioridad durante la noche).

Alta disponibilidad

- PRTG nos da la posibilidad de generar un cluster de alta disponibilidad para un monitoreo de red sin interrupciones.
- Las características son las siguientes:
- En un cluster de PRTG, se pueden combinar hasta 5 instancias ("nodos") para crear un sistema de cluster de alta disponibilidad.
- Ni siquiera una actualización de software causa un periodo de inactividad para un Cluster de PRTG.
- El cluster automáticamente garantiza la alta disponibilidad: si un nodo primario falla o pierde la conexión con el cluster, otro nodo en

seguida toma el papel del servidor principal ("master server") y se encarga de enviar las notificaciones. Así se siguen mandando las notificaciones, incluso si el nodo primario ha perdido su conectividad o ha fallado.

- Además, puede implementar un monitoreo desde varios sitios ("múltiple points-of-presence monitoring"): todos los nodos monitorizan todos los sensores durante todo el tiempo. Eso significa que los tiempos de respuesta se miden desde varios puntos en la red, y los resultados pueden ser comparados entre ellos. Así también se pueden calcular tiempos totales de funcionamiento e inactividad.
- Nos hemos guardado lo mejor para el final: Todas las licencias de PRTG le permiten crear un cluster de alta disponibilidad de dos nodos con solamente una clave de licencia (para 3 o más nodos, necesitará licencias adicionales).

Monitoreo distribuido

Con las sondas remotas ("Remote Probes") PRTG Network Monitor puede supervisar varias redes en diferentes lugares, por ejemplo, para:

- Monitorizar todas las sucursales desde la casa matriz.
- Monitorizar redes separadas en un mismo lugar (p.ej. redes DMZ y LAN).
- Los proveedores de servicios informáticos pueden monitorizar las redes de sus clientes y aumentar la calidad de servicio.
- Para ello, hace falta solamente una instalación núcleo de PRTG ("PRTG Core Server"). Cada licencia de PRTG contiene un número ilimitado de sondas remotas.

Informes detallados

Informes en formato HTMO o PDF

- Los informes se pueden generar ad hoc o de forma programada (cada día, semana, mes).
- Los datos de monitorización históricos se pueden exportar a HTML, XML o CSV.
- PRTG incluye más de 30 plantillas para informes:
- Gráficos y tablas de datos detallados para uno o más sensores.
- Tiempo de funcionalidad / periodos de inactividad (% y segundos).
- Good/failed requests (% y total).
- Top 100 Consumo de ancho de banda.
- Top 100 Uso de CPU.
- Top 100 Tiempos Ping.
- Top 100 Espacio de disco.
- Top 100 tiempo de funcionalidad / periodos de inactividades. (PAESSLER, 2014)

2.2. Marco Conceptual

A continuación, se citan la definición de los términos que más se enmarcan dentro de la investigación planteada:

Bases de Datos: Una base de datos es una colección de información organizada de forma que un programa de ordenador pueda seleccionar rápidamente los fragmentos de datos que necesite (Tecnologicon, 2015).

Firewall: Es una aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles (Tecnologicon, 2015).

Firma antivirus: Una firma antivirus es un archivo que proporciona información al software antivirus para encontrar y reparar los riesgos. Las firmas antivirus proporcionan protección contra todos los virus, gusanos,

troyanos y otros riesgos de seguridad más recientes. Las firmas antivirus también se denominan definiciones de virus (Tecnologicon, 2015).

Gestión de Incidentes: La terminología ITIL define un incidente como: Cualquier evento que no forma parte del desarrollo habitual del servicio y que causa, o puede causar una interrupción del mismo o una reducción de la calidad de dicho servicio (Tecnologicon, 2015).

Incidente de seguridad de información: Evento no deseado o inesperado, que tiene una probabilidad de amenazar la seguridad de la información (Tecnologicon, 2015).

ISO: Norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa (Tecnologicon, 2015).

Malware: El malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer fechorías (Tecnologicon, 2015).

Normas: Término que proviene del latín y significa “escuadra”. Una norma es una regla que debe ser respetada y que permite ajustar ciertas conductas o actividades (Tecnologicon, 2015).

Oficial de seguridad: Persona encargada de administrar, implementar, actualizar y monitorear el Sistema de Gestión de Seguridad de la Información (Tecnologicon, 2015).

Seguridad de la información: La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información

buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma (Tecnologicon, 2015).

Sistema de detección de intrusos: Un sistema de detección de intrusos es un servicio que monitorea y analiza los eventos del sistema para encontrar y proporcionar en tiempo real o casi real advertencias de intentos de acceso a los recursos del sistema de manera no autorizada. Es la detección de ataques o intentos de intrusión, que consiste en revisar registros u otra información disponible en la red. Un sistema de detección de intrusos debe ser parte de una estrategia de seguridad estándar de múltiples niveles (Tecnologicon, 2015).

Sistema de prevención de intrusos: Un sistema de prevención de intrusos es un dispositivo (hardware o software) que supervisa las actividades de la red o del sistema en busca de comportamiento no deseado o malicioso y puede reaccionar en tiempo real para bloquear o evitar esas actividades. Un sistema de prevención de intrusos debe ser parte de una estrategia de seguridad estándar de múltiples niveles (Tecnologicon, 2015).

Vulnerabilidad: Una vulnerabilidad es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad (CIA) de los sistemas (Tecnologicon, 2015). Las vulnerabilidades pueden hacer lo siguiente:

- Permitir que un atacante ejecute comandos como otro usuario
- Permitir a un atacante acceso a los datos, lo que se opone a las restricciones específicas de acceso a los datos
- Permitir a un atacante hacerse pasar por otra entidad
- Permitir a un atacante realizar una negación de servicio

2.3. Marco Normativo

El capítulo I de la (Ley de Servicios de seguridad Privada, 2006) en cuanto a sus disposiciones generales establece en su artículo 1 sobre objeto de ley que:

> Las disposiciones que regulan tanto a las personas naturales y jurídicas públicas o privadas, que prestan servicios de seguridad privada a terceros y aquellas personas jurídicas públicas o privadas que organizan servicios internos por cuenta propia dentro de su organización empresarial; y las actividades inherentes a dicha prestación u organización.

Mientras el artículo 2 que describe el ámbito de aplicación explica que “toda persona natural o jurídica que realiza, en cualquier lugar del territorio nacional, actividades de servicio de seguridad privada bajo modalidad normada en esta Ley, se sujeta a las disposiciones contenidas en la presente Ley”. Más ampliamente el artículo 3 referido a la autoridad competente tiene un impacto importante en el desarrollo de esta investigación dada la relación que posee, con la posibilidad de llevar a cabo esta implementación, puesto que la misma debe regirse por la normativa explicita en adelante:

> **3.1** El Ministerio del Interior es la autoridad competente para la regulación, control y supervisión de los servicios de seguridad privada, en cualquiera de las modalidades normadas en esta Ley. La competencia la ejerce el sector a través de la Dirección General de Control de Servicios de Seguridad, Control de Armas, Municiones y Explosivos de Uso Civil, en adelante DICSCAMEC.
>
> **3.2** La DICSCAMEC en su rol de control y supervisión, realiza acciones inopinadas y aleatorias de control y supervisión de las empresas dedicadas exclusivamente a prestar servicios de seguridad privada; labor que a requerimiento de DICSCAMEC, y de forma específica, puede efectuar la Policía Nacional del Perú, la

misma que al finalizar dicha labor, debe presentar un informe a la DICSCAMEC sobre las actividades realizadas.

3.3 Toda mención que se realice en la presente Ley referida a autoridad competente se entiende por DICSCAMEC.

Cabe mencionar lo descrito en los subcapítulo VI y VII de la Ley de Servicios de seguridad Privada, referido a la prestación de servicios de tecnología de seguridad y prestación de servicios de asesoría y consultoría la cual reza en sus artículos 20 sobre tecnología de seguridad que esta responde a:

> Aquellos servicios prestados por empresas especializadas, cuya actividad comprende los servicios de monitoreo de señales y de respuesta a las mismas, emanadas por dispositivos electrónicos de alarmas; controles de acceso; circuitos cerrados de televisión; sistemas de posicionamiento satelital; y, sistemas de control de mercadería.

Por su parte el artículo 21 inherente a servicios de asesoría y consultoría los define como “aquellos servicios prestados por personas naturales o jurídicas dedicadas a la elaboración de estudios profesionales de seguridad privada, análisis de riesgos, planes de contingencia, evacuación de instalaciones y controles de pérdidas, destinados a optimizar la calidad de la seguridad”.

2.4. Marco Metodológico

Este es un proyecto que uso la investigación descriptiva, porque busco especificar las propiedades, las características y perfiles de la tecnología que se somete a análisis. La misma se encontró enmarcada en un diseño cuasi experimental, dada la necesidad de poner en práctica las simulaciones de red, diseñadas por el investigador para probar las propiedades y procesos principales de la tecnología.

Es importante destacar que el alcance de esta acción es la de configurar en un servidor el sistema de monitoreo a través del software

PRTG para que se realice el monitoreo. A la vez que se presenta la manera de como añadir nuevos puntos y configurar alarmas de manera que el sistema sea versátil y escalable para los usuarios.

Para llevarlo a cabo se realizó un monitoreo por semana como ejemplo del funcionamiento del sistema y de la efectividad que esta realiza. Solo se instalará en un servidor central y los usuarios podrán acceder mediante la red, cualquier problema presentando con la red interna de la empresa o algún bloqueo del sistema tendrá que ser solucionado por la empresa para que el sistema funcione sin inconvenientes.

Es pertinente mencionar que, el SNMP trabaja en la capa de aplicación. El agente SNMP recibe peticiones por el puerto UDP 161. Él debe enviar peticiones desde cualquier puerto disponible de la fuente hacia el puerto 161 del agente. La respuesta del agente será enviada de regreso por el puerto fuente del gestor.

De allí que el gestor recibe notificaciones (Traps e InfofmRequests), sobre el puerto 162. El agente puede generar notificaciones desde cualquier puerto disponible. La idea es que SNMP sea un componente integral y esencial de todos los sistemas TCP/IP, por ello, todos los protocolos por debajo del nivel de aplicación tienen sus componentes SNMP.

SNMP también se ha extendido para cubrir equipos no TCP/IP y algunos protocolos propietarios, constituyéndose en el estándar más ampliamente utilizado para la recogida de información de gestión de red. La idea básica es que la recogida y gestión de la información de la red se haga en las llamadas estaciones de gestión de red que se comunicarán con el resto de los elementos de red.

Estas estaciones de gestión de red serán normalmente estaciones de trabajo que muestran gráficamente aspectos relevantes acerca de los elementos que está monitorizando. La aplicación que se encarga de la comunicación con los elementos de red es el gestor que es la implementación en la estación del protocolo SNMP.

Los elementos de red pueden ser cualquier dispositivo de la red (clásicamente que use parte del conjunto de protocolos TCP/IP) como un router, un terminal, una impresora, etc. Tendremos un software en el elemento de red monitorizado que se denominará agente y cuya función es, por un lado, recoger información de los eventos que se producen en el dispositivo, y por otro comunicarse con el gestor. La comunicación puede producirse de dos maneras:

1. El gestor puede preguntar al agente acerca del valor de alguna variable.
2. El agente puede informar al gestor acerca de algún hecho importante.

En tal sentido, llevar a término esta investigación requirió de una metodología adecuada la cual se explica a continuación:

Tipo de Investigación

Descriptiva

Puesto que, para esta investigación, se obtuvo una entrevista con el Administrador de la red de la empresa Netsecure Perú. El administrador describió las dificultades que tiene para gestionar los dispositivos de comunicaciones centrales y de los servidores ya que se encuentran en dos sedes distintas, por lo que se definió que dispositivos, servicios y servidores deben ser monitoreados de forma constante.

Para tal problemática, se establecieron algunas de las características que debería cumplir la aplicación que realizaría estas tareas. Es necesario explicar que una investigación descriptiva es según (Arias, 2012) la investigación descriptiva consiste en la caracterización de un hecho, fenómeno, individuo o grupo, con el fin de establecer su estructura o comportamiento. Los resultados de este tipo de investigación se ubican en un nivel intermedio en cuanto a la profundidad de los conocimientos se refiere.

Así mismo puede decirse que esta investigación presento una modalidad factible dada sus características puesto que esta es descrita como el tipo de investigación que: Del mismo modo, Arias (2006) señala: “Que se trata de una propuesta de acción para resolver un problema practico o satisfacer una necesidad. Es indispensable que dicha propuesta se acompañe de una investigación, que demuestre su factibilidad o posibilidad de realización”. (p. 134).

Diseño de Investigación

Cuasi Experimental

Para esta investigación se utilizaron algunos de los dispositivos en producción del data center de la organización como son routers, switches, access points y Servidores, que serán configurados en un entorno real de acuerdo a la topología presentada por la organización Netsecure Perú. Lo que la convierte en una investigación bajo el diseño cuasi experimental, que según (Arias, 2006, p. 134).

Método Utilizado

Método Empírico

Su aporte al proceso de investigación es resultado fundamentalmente de la experiencia. Estos métodos posibilitan revelar las relaciones esenciales y las características fundamentales del objeto de estudio, accesibles a la detección sensoperceptiva, a través de procedimientos prácticos con el objeto y diversos medios de estudio (Definicionesabc, 2012).

Objeto:

Datacenter de la Organización.

Medio:

Referencias electrónicas

Pruebas con dispositivos dentro de la red
Recopilación de información bibliográfica

Características del Método Empírico

Las principales características de una investigación empírica son las siguientes:

- Posee una serie de etapas establecidas de antemano que deben ser seguidas para lograr una investigación exitosa.
- Aunque posee una serie de etapas preestablecidas que deberían seguirse, esto no lo hace ser un tipo de investigación rígida, conserva flexibilidad y adaptabilidad en cuanto a sus normas dependiendo de la situación, el problema, los intereses, objetivos, etc.
- En la investigación están establecidas preguntas que deben ser respondidas.
- Se debe definir la población, comportamiento o fenómeno a estudiar.

Entre los Métodos Empíricos se encuentran:

El Método de la Observación Científica

Fue el primer método utilizado por los científicos y en la actualidad continúa siendo su instrumento universal. Permite conocer la realidad mediante la sensopercepción directa de entes y procesos, para lo cual debe poseer algunas cualidades que le dan un carácter distintivo Su aporte al proceso de investigación es resultado fundamentalmente de la experiencia.

Estos métodos posibilitan revelar las relaciones esenciales y las características fundamentales del objeto de estudio, accesibles a la detección sensoperceptiva, a través de procedimientos prácticos con el objeto y diversos medios de estudio, Definicionesabc, (2012).

La Observación Científica debe ser:

- **Consciente. -** Orientado hacia un objetivo o fin determinado.
- **Planificada. -** En función de los objetivos y teniendo en cuenta las condiciones, los medios, el objeto y el sujeto de la observación.
- **Objetiva. -** Despojada lo más posible de subjetividad. Apoyada en juicios de realidad y no en juicios de valor.

El Método de la Medición. - Es el Método Empírico que se desarrolla con el objetivo de obtener información numérica acerca de una propiedad o cualidad del objeto, proceso o fenómeno, donde se comparan magnitudes medibles conocidas. Es la asignación de valores numéricos a determinadas propiedades del objeto, así como relaciones para evaluarlas y representarlas adecuadamente. Para ello se apoya en procedimientos estadísticos, Definicionesabc, (2012).

Método Experimental. - Es el más complejo y eficaz de los métodos empíricos. En este método el investigador interviene sobre el objeto de estudio modificando a esta directa o indirectamente para crear las condiciones necesarias que permitan revelar sus características fundamentales y sus relaciones esenciales, bien sea:

- Aislando al objeto y las propiedades que estudia de la influencia de otros factores
- Reproduciendo el objeto de estudio en condiciones controladas.
- Modificando las condiciones bajo las cuales tiene lugar el proceso o fenómeno que se estudia, Definicionesabc, (2012).

CAPITULO 3: DESARROLLO DEL PROYECTO

3.1. Desarrollo

El presente capitulo aborda la implementación del sistema de monitoreo utilizando el equipamiento disponible de Netsecure Perú (Servidores disponibles para el PRTG); se instalará el software de monitorización PRTG Network Monitor, se configurará los diferentes tipos de sensores para cada dispositivo que se encuentre alojado en el Data center.

PRTG Network Monitor es un sistema de monitorización de Ethernet que le ayuda a tener perfectamente controlado todo lo que ocurre en la red de su empresa. La monitorización de Ethernet no solo incluye la comprobación de la presencia de cortes en los dispositivos de la red, sino que también monitoriza el rendimiento de la red y el uso de sus recursos.

PRTG es un sistema de monitorización de servidores y de red que puede detectar y reaccionar automáticamente ante amenazas y problemas en el rendimiento a tiempo real. También le ofrece ayuda para prevenir posibles fallos en el futuro. Sus funciones incluyen la monitorización de errores y de disponibilidad, asegurando así que todos los dispositivos Ethernet están actualizados, en funcionamiento y registrando la actividad de la red.

3.1.1 Requisitos de Software

- PRTG puede instalarse en versiones de Windows Server o incluso en Windows cliente.

La versión actual del Software PRTG permite su instalación en las siguientes versiones de Windows:

- Windows Server: 2016, 2012 R2 (Recomendada), 2012,2008R2, 2008 (No Recomendada).
- Windows Cliente: Windows 10, Windows 8.1, Windows 8 (No recomendada).

- También se requiere. NET Framework 4.5 o posterior con los últimos parches, a partir de Windows Server 2012 y Windows 8, ya se integran estas versiones de .NET en el sistema operativo.
- Para acceder a la interfaz web, la versión actual del PRTG requiere utilizar alguna de las siguientes versiones: Google Chrome 67 o posterior (Recomendado), Mozilla Firefox 61 o posterior, Internet Explorer 11.

3.1.2 Requisitos de Hardware

Dependerán principalmente de los tipos de sensores y los intervalos que serán aplicados a cada dispositivo.

- CPU: un servidor con al menos una CPU de doble núcleo
- Memoria Ram: Requisito mínimo: 2048 MB de RAM. Necesitas unos 150 KB de RAM por sensor
- Unidad de disco duro: Necesita aproximadamente 200 KB de espacio en disco por sensor por día (para sensores con un intervalo de 60 segundos).

3.1.3 Implementación del servidor PRTG

Para la implementación del servidor PRTG se toma en cuenta las recomendaciones del fabricante. Uno de los beneficios grandes que se tiene para este proyecto es que la organización Netsecure Perú cuente con un servidor IBM System X3550 con procesador Intel Xeon E5405 Quad-Core, memoria de 8 GB 667 MHz y con una capacidad de 500 GB, cuenta con características superiores a lo recomendado y sobre todo se encuentra en buen estado, sin uso por motivo de que el sistema CRM (Sistema de gestión de clientes) que se encontraba funcionando se dio de baja y fue migrado por un sistema más completo (DatCorp ERP), lo que tiene como beneficio el ahorro de adquirir un nuevo servidor.

Para ello se utilizará un sistema operativo Microsoft Windows Server 2012 R2 para obtener el mejor rendimiento y un navegador web para acceder a la interfaz web como Google Chrome versión 73. A continuación, en los siguientes puntos se detallan el proceso para su implementación. Hay muchos parámetros que influyen en el rendimiento y la estabilidad de PRTG. Para la gran mayoría de los usuarios de PRTG recomendamos lo siguiente en cuanto al tamaño para el hardware del servidor PRTG.

3.1.4 Resumen de las Configuraciones recomendadas

Le recomendamos que haga funcionar el servidor central de PRTG así como todas las sondas remotas:

- Con hardware x64 de PC/Server
- Con Windows Server 2012 R2, Windows Server 2016 o Windows 10.
- Que tenga instalado .NET Framework 4.7.2 o posterior.

Hay muchos parámetros que influyen en el rendimiento y la estabilidad de PRTG. Para la gran mayoría de los usuarios de PRTG recomendamos lo siguiente en cuanto al tamaño para el hardware del servidor PRTG.

Sensores por servidor central	Licencia	Hardware del servidor central recomendado	Espacio de disco (1 año retención de datos)	Cuentas de usuario	Sondas remotas	Virtualización	PRTG Cluster
Hasta 1.000 sensores (~ 100 dispositivos)	PRTG 1000	2 CPU Cores, 3 GB RAM	250 GB	< 30	< 30	✓	✓
1.000 - 2.500 sensores (~ 250 dispositivos)	PRTG 2500	3 CPU Cores, 5 GB RAM	500 GB	< 30	< 30	✓	✓
2.500 - 5.000 sensores (~ 500 dispositivos)	PRTG 5000	5 CPU Cores, 8 GB RAM	1 TB	< 20	< 30	✓	!
5,000 - 10,000 sensores (~ 1.000 dispositivos)	PRTG XL1	8 CPU Cores, 16 GB RAM	2 TB	< 10	< 30	! *	!
Más de 10.000 sensores	Recomendamos configurar instalaciones adicionales del servidor central de PRTG y que contacte a nuestro equipo de preventas.						

Figura 11. Configuración recomendada

Fuente: PAESSLER (2019)

3.2. Pasos a seguir para la instalación del PRTG

A continuación, se describirá el proceso mediante el cual se realizó la implementación de la solución diseñada. La descripción incluye imágenes paso a paso del procedimiento:

3.2.1 Descargar producto

Se descargó la última versión de la aplicación disponible desde el sitio web de Paessler

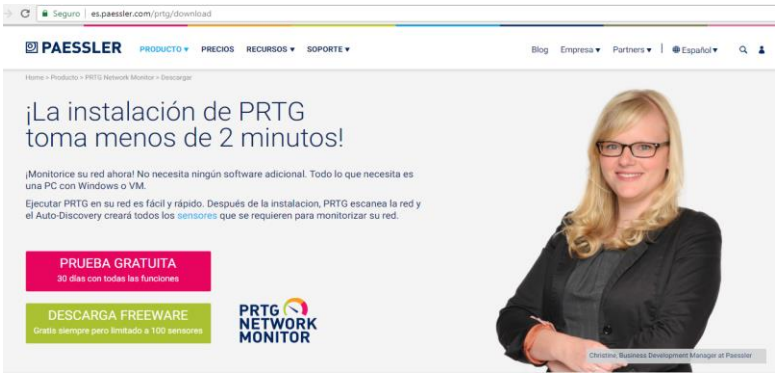

Figura 12. Proceso de descarga de Aplicación

Fuente: PAESSLER (2019)

3.2.2 Ejecutar el archivo de instalación

Una vez que haya finalizado la descarga, en el Escritorio del servidor se encontrará el instalador que indica que ya es posible iniciar la instalación.

Figura 13. Finalización de la descarga del aplicativo

Fuente: Netsecure Perú (2019)

3.2.3 Ejecutar el archivo de instalación

Se procede con la ejecución del instalador y se continúa con las instrucciones indicadas.

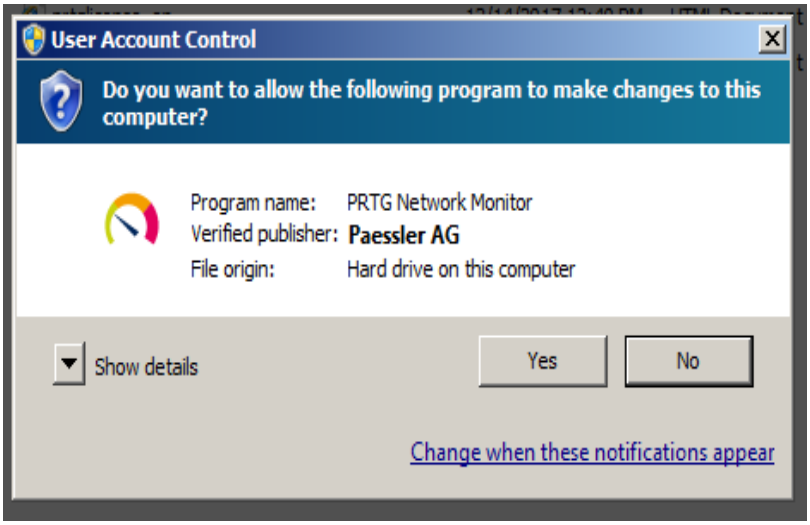

Figura 14. Ejecución del instalador

Fuente: Netsecure Perú (2019)

3.2.4 Se acepta el acuerdo de licencia

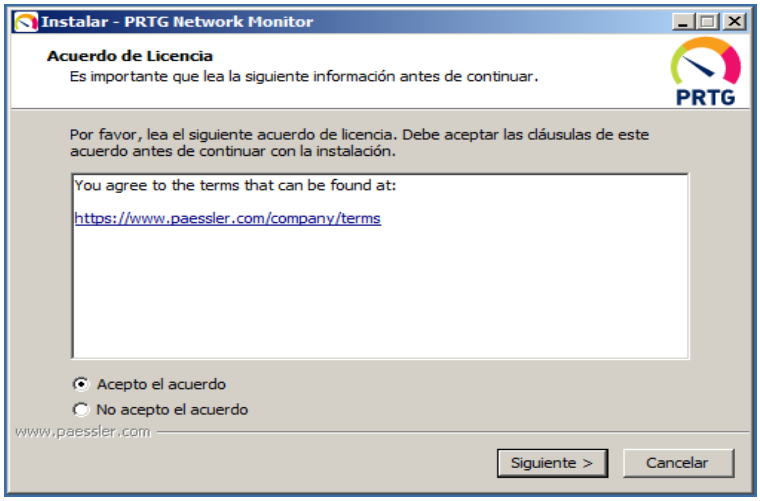

Figura 15. Acuerdos de licencia

Fuente: Netsecure Perú (2019)

3.2.5 Se coloca el correo del Administrador

Se ingresa la cuenta de correo del personal encargado el servidor PRTG enviará alertas importantes a esta cuenta de correo.

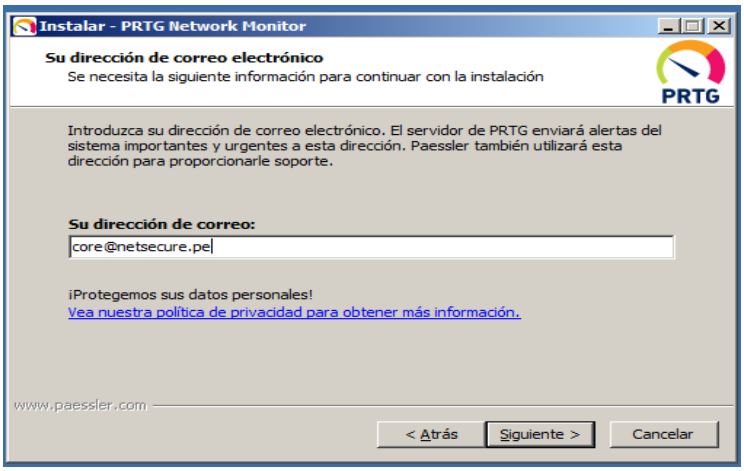

Figura 16. Configuración de la cuenta del administrador

Fuente: Netsecure Perú (2019)

3.2.6 Configuración de Licencia

Se ingresa la licencia que adquirimos a Paessler, se debe proporcionar el Nombre y la Clave de licencia exactamente como se recibió al correo electrónico.

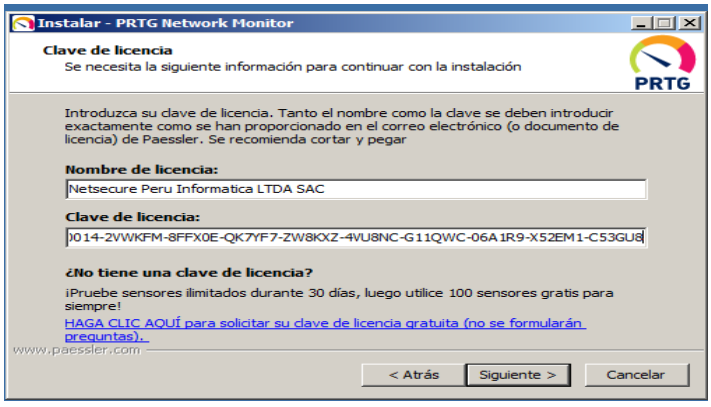

Figura 17. Información clave de licencia

Fuente: Netsecure Perú (2019)

3.2.7 Reconocimiento de Licencia

En este proceso se valida la licencia que fue adquirida con los servidores de Paessler.

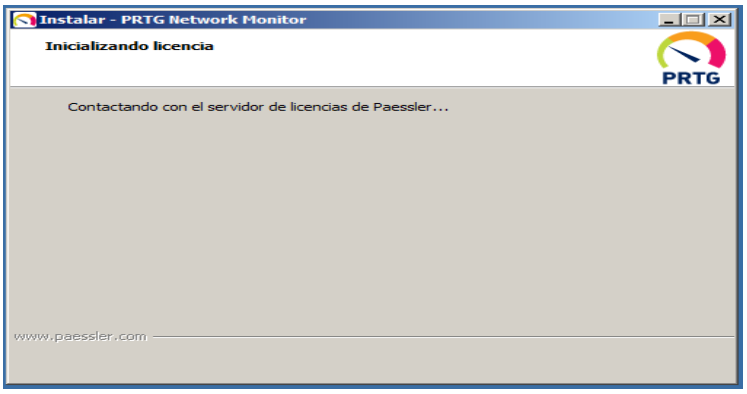

Figura 18. Validación de licenciamiento de aplicativo

Fuente: Netsecure Perú (2019)

3.2.8 Instalación del Software PRTG

Se procede con la instalación del aplicativo en la partición C del disco duro.

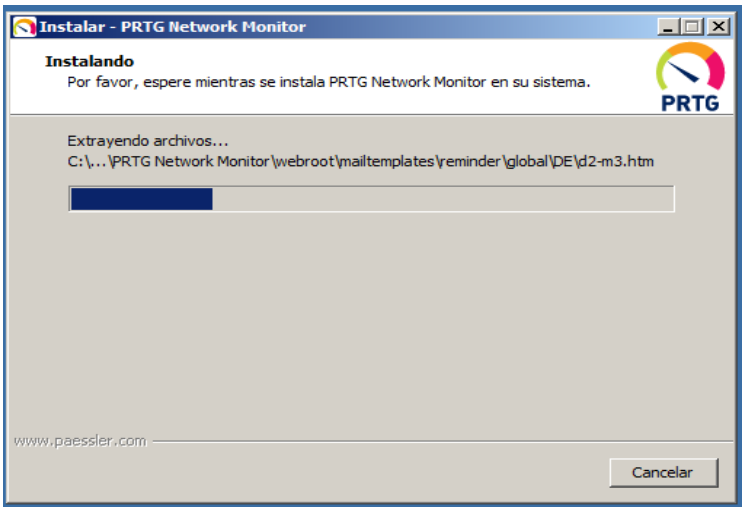

Figura 19. Selección de la carpeta de instalación

Fuente: Netsecure Perú (2019)

3.2.9 Finalización de la Instalación

Luego de finalizar la instalación, PRTG abre la Interfaz Web Ajax en el navegador predeterminado de su sistema utilizando la dirección IP privada que se le asignó al servidor, introducimos el usuario y contraseña de administración de PRTG, por defecto es prtgadmin, e iniciamos sesión.

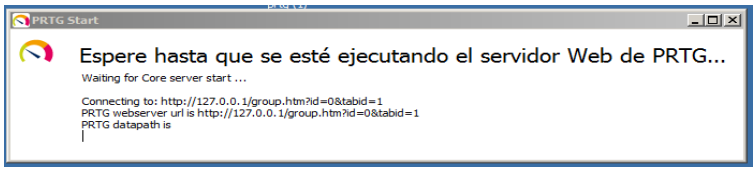

Figura 20. Ejecución del Servidor Web

Fuente: Netsecure Perú (2019)

Figura 21. Inicio de la aplicación

Fuente: Netsecure Perú (2019)

3.3. Configuración del PRTG

Dicha configuración es requerida para la administración de la herramienta y él envió de notificaciones por medio del correo electrónico.

3.3.1. Cuentas de Usuario

Para la creación de una cuenta de usuario con privilegios de administrador, ingresamos a configuración, Administración del sistema y se

ingresa a cuentas de usuario, se agrega una cuenta del usuario Administrador.

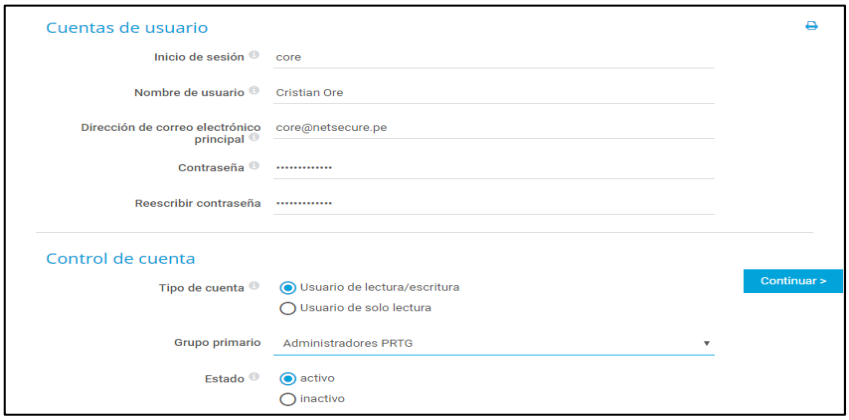

Figura 22. Configuración cuenta del administrador

Fuente: Netsecure Perú (2019)

3.3.2. Configurar Servidor de correo

Es uno de los métodos que utiliza para notificar a través de un mensaje de correo electrónico, para este escenario se utiliza el recomendado que es configurando un servidor relay SMTP.

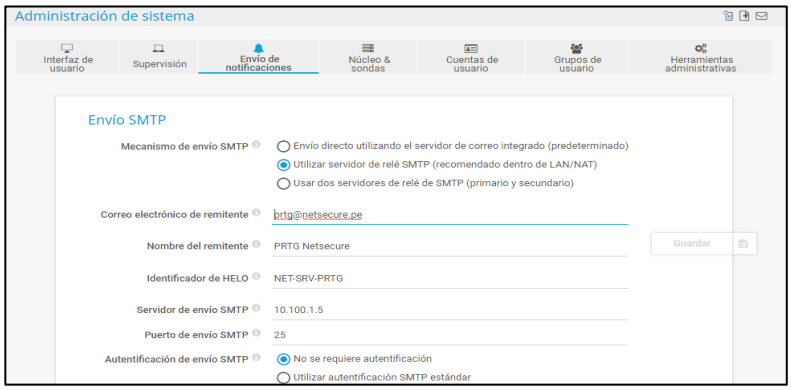

Figura 23. Configurador del servidor relay SMTP

Fuente: Netsecure Perú (2019)

3.4. Configuración de Grupos, Aparatos y sensores

El servidor PRTG se encuentra lista para iniciar el monitoreo de la red y los servicios de Netsecure Perú, en esta sesión se describirá paso a paso el proceso de los grupos, aparatos y sensores a monitorear.

3.4.1. Configuración de los Grupos

Se debe crear dos grupos para organizar objetos similares y así poder facilitar la herencia de la configuración de los mismos, dentro del grupo creado por defecto con nombre Sonda con click derecho procedemos añadir el grupo Netsecure y luego procederemos con la creación del grupo Netsecure San Isidro y Netsecure Villa el Salvador, quedando tal y como se muestra en la imagen

Figura 24. Agregando Grupos

Fuente: Netsecure Perú (2019)

3.4.2. Configurar protocolo SNMP en Windows Server

Para iniciar el monitoreo a uno de los servidores, se agregará un servidor principal que se encuentra con Windows Server 2012 R2, para ello tendremos que instalar el protocolo SNMP. Abrir la herramienta

ServerManager.exe y situarnos sobre la opción: Administrar y pulsar sobre: Agregar roles y características.

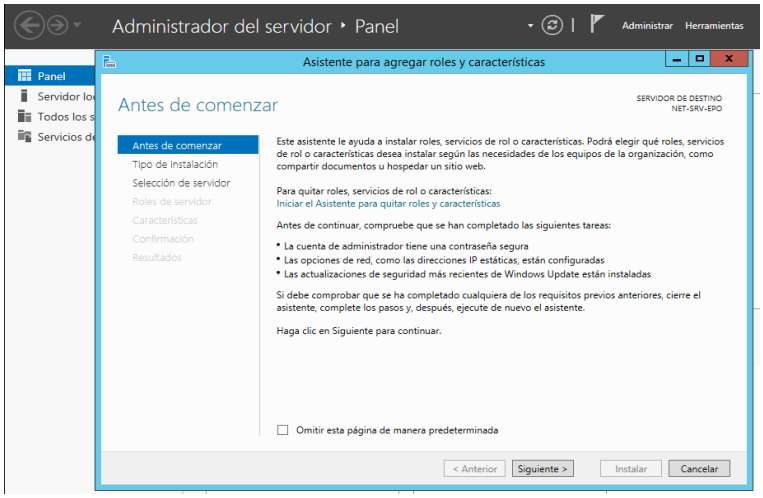

Figura 25. Instalar SNMP en Windows Server

Fuente: Netsecure Perú (2019)

A continuación, seleccionamos la opción: Instalación basada en características o en roles.

Figura 26. Asistente para agregar características

Fuente: Netsecure Perú (2019)

Se selecciona el servidor NET-SRV-EPO en el que se instalara el rol

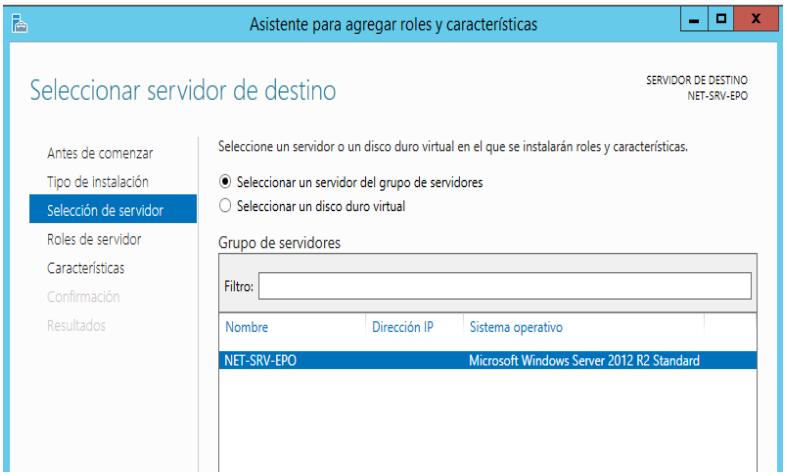

Figura 27. Seleccionar servidor para instalar característica

Fuente: Netsecure Perú (2019)

Dentro de las características se encuentra el protocolo SNMP como servicio, se selecciona el Proveedor WMI para SNMP, ya que esto permitirá desde PRTG lanzar scripts que ejecuten consultas WMI

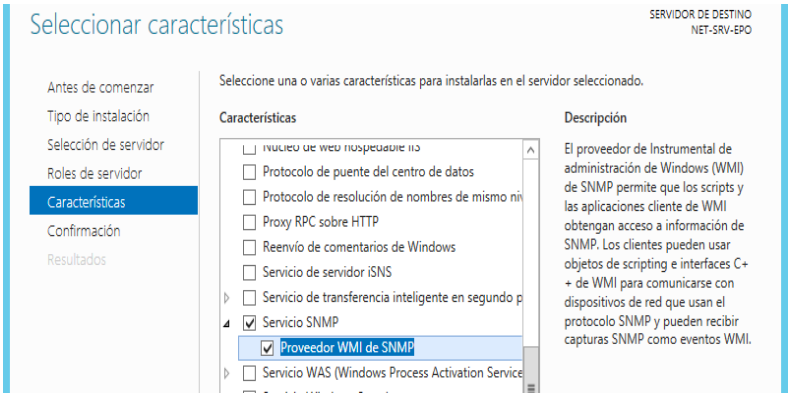

Figura 28. Seleccionar las características

Fuente: Netsecure Perú (2019)

Se confirman las opciones seleccionadas en el asistente y procedemos con la instalación.

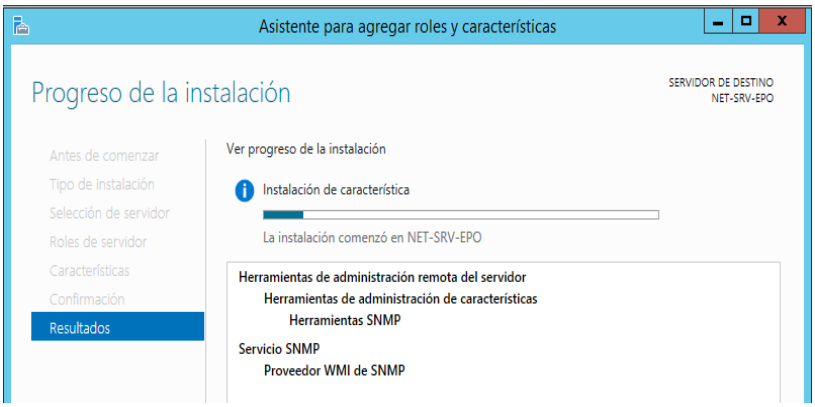

Figura 29. Instalando características WMI de SNMP

Fuente: Netsecure Perú (2019)

Para configurar SNMP en el servidor, nos dirigirnos a la consola de administración de servicios: services.msc, ingresamos a Servicio SNMP en el menú seguridad puede configurarse la comunidad SNMP y la dirección IP del Servidor PRTG para poder leer los paquetes SNMP.

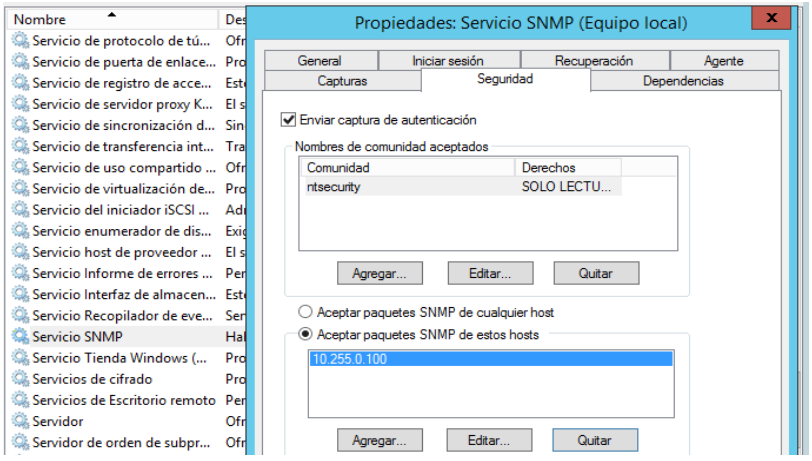

Figura 30. Configurar comunidad SNMP

Fuente: Netsecure Perú (2019)

3.4.3. Configuración de los equipos

Cabe indicar que para monitorear cualquier dispositivo esta debe pertenecer a la red del servidor, en el menú dispositivos hacemos click sobre añadir dispositivo.

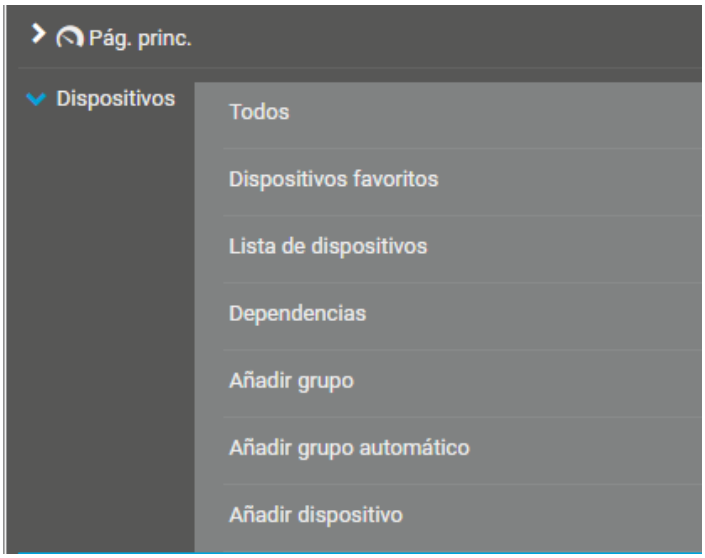

Figura 31. Agregar dispositivo

Fuente: Netsecure Perú (2019)

Se indica el nombre del servidor y se señala la IP servidor que se quiere monitorizar vía SNMP.

Figura 32. Configuración del nuevo dispositivo

Fuente: Netsecure Perú (2019)

El sistema PRTG permite realizar de varias formas el escaneo de los sensores, para tener una gestión controlada de este proceso se selecciona la opción para ejecutar el escaneo solamente cuando sea necesario.

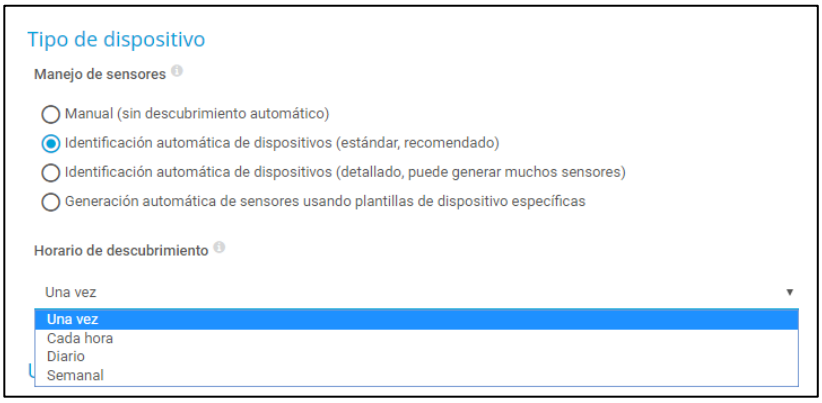

Figura 33. Configuración Horario de descubrimiento

Fuente: Netsecure Perú (2019)

Para finalizar el servidor ya se encuentra en red y operativo tal y como figura en la consola PRTG.

Figura 34. Configuración de un nuevo equipo

Fuente: Netsecure Perú (2019)

3.4.4. Configuración de Sensores

Una vez que se ha añadido el dispositivo, se procede a añadir el sensor, el primer sensor que automáticamente se debe agregar es el de tiempo de actividad o Ping, se pulsa sobre el servidor y se hace click en añadir sensor.

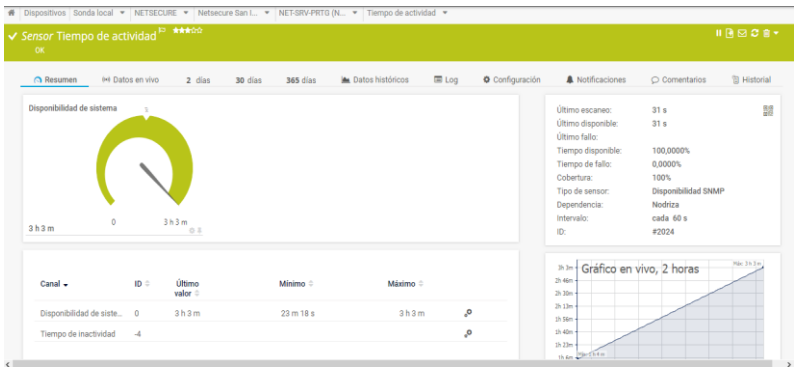

Figura 35. Vista de sensor monitoreando servidor

Fuente: Netsecure Perú (2019)

Se puede ir añadiendo sensores de CPU, Memoria, Capacidad y actualizaciones de Windows de la siguiente manera:

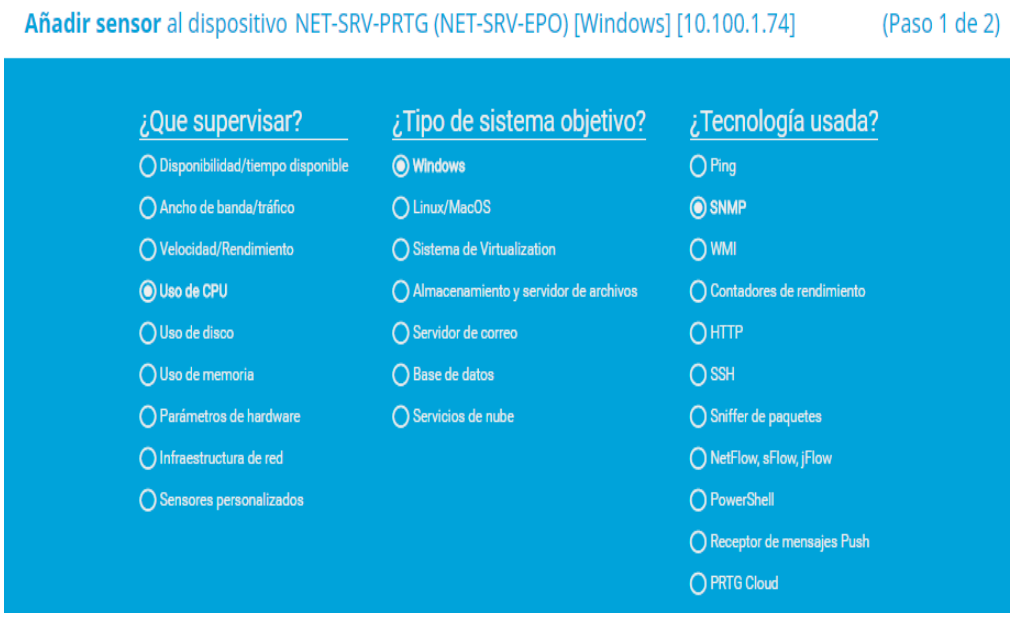

Figura 36. Selección de tipo de sensores

Fuente: Netsecure Perú (2019)

Tipo de sensor correspondiente

Figura 37. Sensor de carga de CPU

Fuente: Netsecure Perú (2019)

3.5. Configuración de notificación

Las notificaciones se configuran directamente sobre cada sensor, cada uno registra cierta información diferente, para habilitar notificaciones

de alertas de SNMP tendremos que ingresar a un dispositivo para este escenario se elegirá un sensor de CPU.

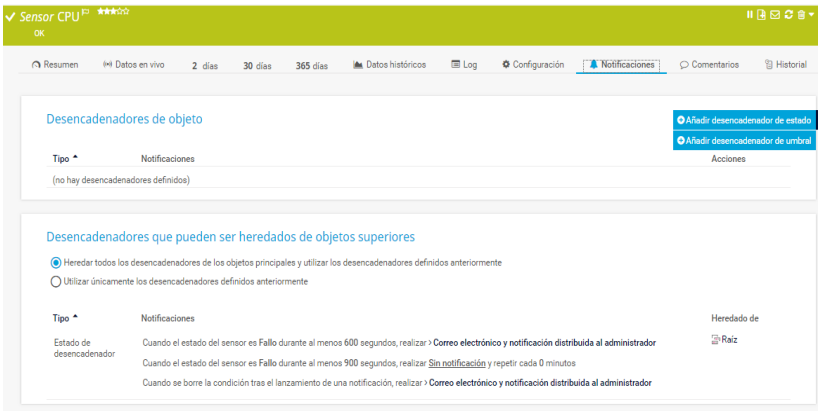

Figura 38. Configuración de activación de notificación

Fuente: Netsecure Perú (2019)

Se agrega un disparador de umbral, este disparador se activará cuando un sensor alcanza valores específicos, para este caso si el total de CPU está por encima del 80% envíe un correo al administrador y cuando esta condición finalice informe nuevamente.

Figura 39. Disparadores de objetos

Fuente: Netsecure Perú (2019)

Si la notificación es configurada correctamente, llegara un correo con la siguiente alerta: Umbral alcanzado con 80% de carga de CPU

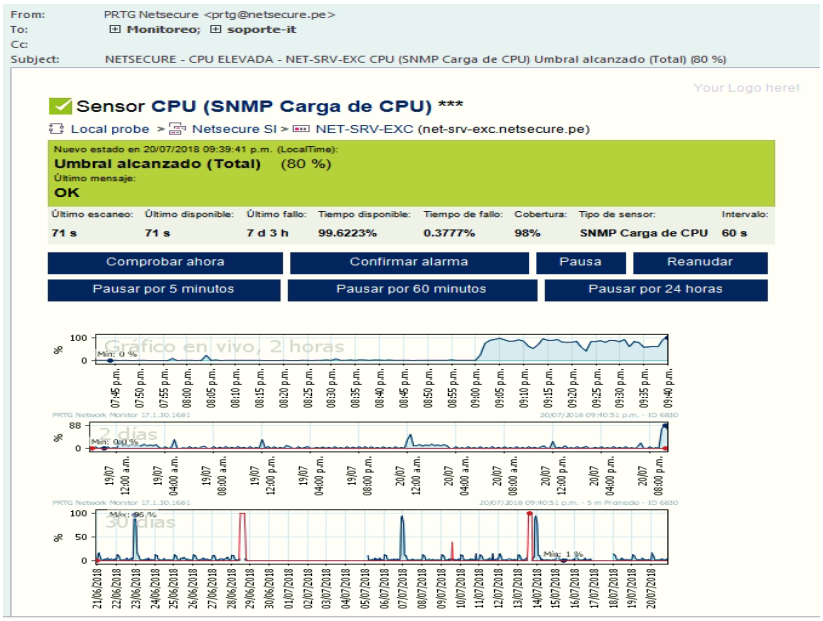

Figura 40. Recepción de alerta de correo carga CPU

Fuente: Netsecure Perú (2019)

Si la carga de CPU se logra restablecer y esta se encuentra por debajo de los 80% llegara un correo con la siguiente alerta: Alarma Liberada de Carga de CPU.

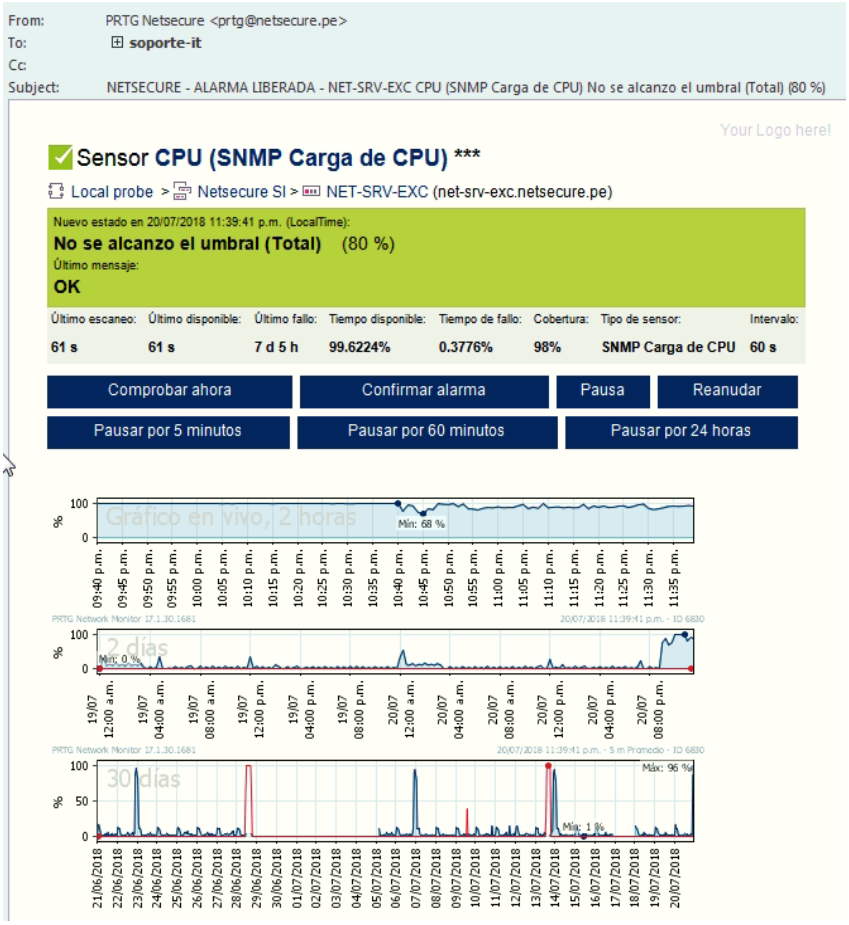

Figura 41. Recepción de alerta de correo alarma liberada

Fuente: Netsecure Perú

3.6. Configuración de la comunidad SNMP

Para usar la cadena de comunidad y desplegar a todos los grupos, simplemente configuramos la comunidad en el objeto Raíz, dentro de la pestaña de configuración se ubica las credenciales para dispositivos SNMP, se configura como requerido / deseado.

Cabe mencionar que las credenciales de SNMP serán heredadas por todos los objetos por debajo del nivel donde fue configurado.

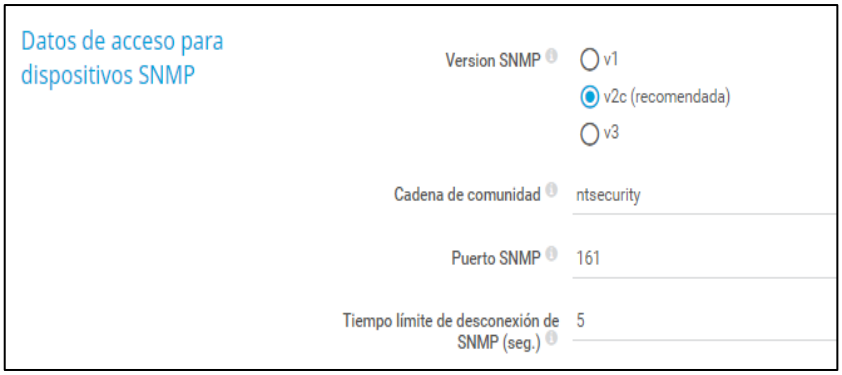

Figura 42. Acceso para dispositivo SNMP

Fuente: Netsecure Perú

3.7. Ventajas de usar PRTG para supervisar el rendimiento del servidor

- **Mantener la vista en el hardware**

PRTG proporciona una visión general constante de todo su hardware que se puede utilizar con múltiples fabricantes diferentes. Si se supera un determinado valor, se le notificará de inmediato; normalmente, antes de que las cosas se pongan serias. Esto le ahorrará tiempo y estrés en su trabajo cotidiano.

- **Identificar cuellos de botella**

La supervisión de PRTG le permite detectar los cuellos de botella rápidamente, a menudo antes de que surjan problemas. Esto significa que puede actuar de forma rápida y proactiva para mantener su servidor en funcionamiento e, incluso, mejorarlo.

- **Información histórica**

PRTG le proporciona datos históricos durante un período de tiempo prolongado. Estos datos le permiten ver si su red se sobrecarga, y en qué medida. Los informes personalizados y los gráficos generados automáticamente ayudan con la documentación.

- **Transversal**

Además de la supervisión de redes locales, PRTG es especialmente adecuado para las redes distribuidas. Las sondas remotas de PRTG supervisan los servidores en diferentes lugares desde una ubicación centralizada, lo que reduce su necesidad de desplazamientos.

- **Rendimiento De Todo Tipo**

PRTG le permite supervisar todos los tipos de rendimiento de sus servidores. No importa si dispone de 4 o 60 GB de RAM. Las licencias de PRTG se pueden actualizar para satisfacer sus propias necesidades específicas. Las redes pequeñas pueden utilizar la versión introductoria de PRTG, que viene con 100 sensores gratuitos.

- **Los Principales Fabricantes**

PRTG es compatible con los principales proveedores de servidores. Por lo tanto, puede supervisar todo su parque de terminales/servidores con una sola herramienta de supervisión centralizada, ahorrando mucho tiempo y energía en lo que respecta a la gestión del sistema.

CAPITULO 4: ANALISIS DE COSTO Y BENEFICIO

4.1. Análisis de Costos

El análisis de costos se va a detallar todos aquellos costos que se van a tener en cuenta para el desarrollo del proyecto e incluyen los costos de equipos, costos de materiales, Costos de recursos humanos. Por consiguiente, la obtención del valor económico de este plan de negocio es importante considerar las características del jefe de proyecto, quien debe desempeñar habilidades en la comprensión del lenguaje PRTG, asiento de datos, configuraciones SNMP, preparación en el manejo de diferentes sistemas operativos, protocolos de red, manejo y administración de los sistemas operativos, así como de otras acciones inherentes. Debido a la complejidad del proyecto se plantea el requerimiento de que el grupo de trabajo posea suficientes capacidades en la ejecución de actividades en este sector, en este caso 3 personas.

- Duración del proyecto: 3 meses
- Horas invertidas por día: 8
- Días laborados por semana: 5
- Semanas laboradas por mes: 4
- Recursos humanos: 3

Se trabajará alrededor de 20 días por mes. Por lo que el total de horas trabajadas en este proyecto será de:

$$\frac{20\ dias}{[mes]} * \frac{8\ [hrs]}{[dia]} * 3\ [meses] * 3\ [personas]$$
$$= 1{,}440\ [horas]$$

Obteniendo un valor de 25 Soles cada hora aproximadamente, el costo total del recurso humano utilizado en este proyecto sería de 35,400 Soles.

4.1.1. Costo de Recursos Humanos

En este punto se identificará cuanto puede costar la implementación del proyecto en base al equipo que se conformara para tal fin, en el caso de la empresa Netsecure Perú el personal que realizara el trabajo es personal interno por lo mismo simularemos cuanto podría costar contratar un equipo de trabajo detallo:

Jefe del Proyecto

Es el profesional que se encargará de asegurar que el proyecto se cumpla al 100 % esperado, cumpliendo los márgenes de tiempo establecidos y los costos esperados para el buen desarrollo. La participación del jefe de proyecto es integra quien sustentara los costos estimados durante el tiempo de duración que tiene el proyecto en ejecución. Percibirá un sueldo mensual de S/6,000 por un periodo de 6 meses de servicio.

Administrador de Red

Es el profesional que se encargará de realizar todo el análisis, diseño, instalación y configuración de la implantación del software de monitoreo en la organización, que trabajará desde el inicio del proyecto. Dicho profesional deberá como responsable del proyecto instalar y configurar el servidor donde se instalará el software PRTG, deberá realizar las configuraciones de los sensores de cada dispositivo, así como también las alertas y notificaciones y otras configuraciones que se requieran para el correcto funcionamiento. Percibirá un sueldo mensual de S/. 3,000 por un periodo de 3 meses de servicio.

Soporte técnico

Es el profesional que se encargará de añadir cada dispositivo que se encuentra en el datacenter, y agregar los sensores correspondientes para analizar los recursos del dispositivo. Es el personal de apoyo durante la implantación del proyecto. Percibirá un sueldo de S/. 1,800 por un periodo de 3 meses de servicio.

Tabla 2. Costo por recursos humanos

Concepto	Cantidad	Tiempo (MESES)	Costo (Mensual)	Importe
Jefe de Proyecto	1	3	S/. 7,000.00	S/. 21,000.00
Administrador de Red	1	3	S/. 3,000.00	S/. 9,000.00
Soporte Tecnico	1	3	S/. 1,800.00	S/. 5,400.00
			Costo Total por Recursos Humanos (S/.):	**S/. 35,400.00**

Fuente: Netsecure Perú (2019)

4.1.2. Costo de Equipos

Para la elaboración del Proyecto va a ser necesario la adquisición:

Servidor:

Se requerirá de la adquisición de un servidor para la implantación del sistema de monitoreo. Actualmente la empresa Netsecure Perú cuenta con 1 servidor disponible para el proyecto, lo cual será incluido en los costos como valor 0 ya que no se realizará ninguna compra de servidores. Se va a incluir una memoria Ram de 8 GB, contar con la memoria RAM suficiente nos permitirá obtener mejor servicio con respecto a las aplicaciones del Software. Asimismo, se incluirá un disco duro de 500 GB con la finalidad de aplicar la configuración de redundancia y tolerancia a fallo (RAID 1).

Tabla 3. Costo por compra de equipos

Cantidad	Descripcion	P.U.($)	Costo ($)
1	Servidor IBM Systema x3650	2,200.00	0.00
1	Memoria 8 GB DDR3 SDRAM - ECC -10600	281.00	281.00
1	Disco duro, 500 GB, SAS 6.0, 7200 RPM, G2 Hot-Swap, 2.5"	600.00	600.00
	Costo Total por Compra de Equipo ($):		**$ 881.00**
	Costo Total por Compra de Equipos (S/.) x 3.32:		**S/. 2,924.92**

Fuente: Netsecure Perú (2019)

Software

Se requerirá la adquisición de 2 licencias, una licencia corresponderá al Sistema Operativo y otra licencia para el PRTG

Tabla 4. Costo por licenciamiento

Concepto	Cantidad	Costo
Licencia Windows Server 2016 R2	1	S/. 2,900.00
Licencia PRTG	1	S/. 5,260.00
Costo Total por Licenciamiento (S/.):		**S/. 8,160.00**

Fuente: Netsecure Perú (2019)

4.1.3. Costo de Mantenimiento

Tabla 5. Costo por mantenimiento

Cantidad	Descripcion	P.U.($)	Costo ($)
	Como existe el personal capacitado en la organización, los costos de mantenimiento seran realizados como una de las funcioines del personal encargado, por tal no se va considerar el costo.	0.00	0.00
	Costo Total por Mantenimiento (S/.):		**0.00**

Fuente: Netsecure Perú (2019)

4.1.4. Resumen del Costo Total

Aquí se indica la inversión que se realizó para el desarrollo de nuestro proyecto expresado en Soles.

Tabla 6. Resumen de costo total

Rubro	Costo ($)
Costo de Equipos	2,924.92
Costo de Software	8,160.00
Costo de Recursos Humanos	35,400.00
Costo de Mantenimiento	0.00
Costo Total (S/.):	**46,484.92**

Fuente: Netsecure Perú (2019)

4.1.5. Financiamiento

El financiamiento viene a ser el medio por a través del cual se conseguirán los recursos para desarrollar el proyecto, estipulándose que, por tratarse de un proyecto privado, el 100% fue musculo económico propio. Cabe mencionar que el costo total de la inversión se ubica en cuarenta y seis mil cuatrocientos ochenta y cuatro soles con noventa y dos céntimos (**46.484,92**).

Tabla 7. Estructura financiera

Estructura Financiera			Préstamo	Capital Propio	Inversión Total
Porcentaje de Apalancamiento	**100**	Propio	**0,00**	**46.484,92 soles**	**Soles 46.484,92**

***Fuente**: Oré, C. (2019)*

Habiendo presentado la estructura financiera se consideró necesario determinar la tasa anual de recuperación de la inversión suponiendo que la misma tenga un monto de 0.26 % establecidos según el crecimiento porcentual financiero de la empresa cada año, y al ser la deuda inicial del posible financiamiento de 46.484,92 soles las cuotas anuales durante 5 años de plazo serán de 9.358,56 soles realizadas en 60 fracciones de 779,88 soles con un incremento mensual del 0.02%.

Tabla 8. Cálculo de amortización de gasto

TASA ANUAL	0,26%
Nº DE FRACCIONES	60
VALOR DE DEUDA	Soles 46.484,92
CUOTAS	Soles 9.358,56
TASA ANUAL	0,26%
TASA MENSUAL	0,02%
Nº DE AÑOS	5
CUOTAS	Soles 779,88
VALOR DE DEUDA	Soles 46.484,92

***Fuente**: Oré, C. (2019)*

Tabla 9. Amortización Mensual

TABLA DE AMORTIZACIÓN(MENSUAL)				
PERIODO	CUOTA	INTERES	AMORTIZACIÓN	CAPITAL VIVO
0				46484.94
1	779.88	10.07	769.81	45715.13
2	779.88	9.90	769.97	44945.16
3	779.88	9.74	770.14	44175.02
4	779.88	9.57	770.31	43404.71
5	779.88	9.40	770.48	42634.23
6	779.88	9.24	770.64	41863.59
7	779.88	9.07	770.81	41092.78
8	779.88	8.90	770.98	40321.80
9	779.88	8.74	771.14	39550.66
10	779.88	8.57	771.31	38779.35
11	779.88	8.40	771.48	38007.87
12	779.88	8.24	771.64	37236.23
13	779.88	8.07	771.81	36464.42
14	779.88	7.90	771.98	35692.44
15	779.88	7.73	772.15	34920.29
16	779.88	7.57	772.31	34147.98
17	779.88	7.40	772.48	33375.50
18	779.88	7.23	772.65	32602.85
19	779.88	7.06	772.82	31830.03
20	779.88	6.90	772.98	31057.05
21	779.88	6.73	773.15	30283.90
22	779.88	6.56	773.32	29510.58
23	779.88	6.39	773.49	28737.09
24	779.88	6.23	773.65	27963.44
25	779.88	6.06	773.82	27189.62
26	779.88	5.89	773.99	26415.63
27	779.88	5.72	774.16	25641.48
28	779.88	5.56	774.32	24867.15
29	779.88	5.39	774.49	24092.66
30	779.88	5.22	774.66	23318.00
31	779.88	5.05	774.83	22543.17
32	779.88	4.88	775.00	21768.18
33	779.88	4.72	775.16	20993.01
34	779.88	4.55	775.33	20217.68
35	779.88	4.38	775.50	19442.18
36	779.88	4.21	775.67	18666.52
37	779.88	4.04	775.84	17890.68
38	779.88	3.88	776.00	17114.68
39	779.88	3.71	776.17	16338.51
40	779.88	3.54	776.34	15562.17
41	779.88	3.37	776.51	14785.66
42	779.88	3.20	776.68	14008.98
43	779.88	3.04	776.84	13232.14
44	779.88	2.87	777.01	12455.12
45	779.88	2.70	777.18	11677.94
46	779.88	2.53	777.35	10900.59
47	779.88	2.36	777.52	10123.08
48	779.88	2.19	777.69	9345.39
49	779.88	2.02	777.85	8567.53
50	779.88	1.86	778.02	7789.51
51	779.88	1.69	778.19	7011.32
52	779.88	1.52	778.36	6232.96
53	779.88	1.35	778.53	5454.43
54	779.88	1.18	778.70	4675.73
55	779.88	1.01	778.87	3896.87
56	779.88	0.84	779.04	3117.83
57	779.88	0.68	779.20	2338.63
58	779.88	0.51	779.37	1559.25
59	779.88	0.34	779.54	779.71
60	779.88	0.17	779.71	0.00

***Fuente**: Oré, C. (2019)*

Por lo que el financiamiento de la empresa Netsecure seria de cuarenta y seis mil cuatrocientos ochenta y cuatro con noventa y dos céntimos (46.484,92) correspondiente al 100% del total de costos por operatividad del sistema de monitoreo.

Tabla 10. Amortización anual

TABLA DE AMORTIZACIÓN (ANUAL)				
PERIODO	CUOTA	INTERES	AMORTIZACIÓN	CAPITAL VIVO
0				46484.94
1	9358.56	109.84	9248.71	37236.23
2	9358.56	85.77	9272.79	27963.44
3	9358.56	61.63	9296.93	18666.52
4	9358.56	37.43	9321.13	9345.39

***Fuente**: Oré, C. (2019)*

4.1.6. Depreciación y Amortización

Al hacer referencia de depreciación o amortización de un activo se hace mención a los activos fijos. En otro sentido: algunos capitales de una empresa, como el inmobiliario, la maquinaria, etcétera, van disminuyendo su valor (se deprecian) y esto ha de suponerse como un gasto**.** En tal sentido, la depreciación fue calculada por el método línea recta, para cada uno de los activos tangibles, valuando entre 5 y 10 años para la vida útil de los mismos y tomando en cuenta el precio al momento de su compra, calculando su depreciación mensual y anual, tal y como se muestra a continuación:

Tabla 11. Depreciación de activos tangibles

MÉTODO CONTABLE								
VALORACION DE ACTIVOS FIJOS PARA UN FLUJO DE 10 AÑOS								
ACTIVO	VALOR DE COMPRA	VIDA CONTABLE	DEPRECIACION ANUAL	REINVERSION EN 10 AÑOS	TOTAL, DE REINVERSIO N	AÑOS DEPRECIANDOS E	DEPRECIACION ACUMULADA	VALOR EN LIBRO
Equipo de Computación	2,924.92	5	584.984	1	2924.92	10	5849.84	-2924.92
Software	8160	5	1632	1	8160	10	16320	-8160
	Depreciación Acumulada		2216.98				Valor de Desecho	0

***Fuente**: Oré, C. (2019)*

De allí que el total en soles de activos tangibles será de 11.044,92 los cuales sufrirán en 10 años una depreciación de 2216.98 soles mientras la amortización de los activos intangibles se refleja de la manera siguiente:

Tabla 12. Amortización de activos intangibles

MÉTODO CONTABLE								
VALORACION DE ACTIVOS FIJOS PARA UN FLUJO DE 10 AÑOS								
ACTIVO	VALOR DE INVERSION	VIDA CONTABLE	DEPRECIACION ANUAL	REINVERSION EN 10 AÑOS	TOTAL, DE REINVERSION	AÑOS DEPRECIANDOSE	DEPRECIACION ACUMULADA	VALOR EN LIBRO
Recursos	35,400.00	1	35400	1	35400	10	354000	-
Humanos								318600
	Depreciación Acumulada		35400				Valor de Desecho	-
								318600

***Fuente**: Oré, C. (2019)*

Cabe destacar que para el cálculo de la depreciación se utilizó la formula presente en la tabla siguiente:

Tabla 13. Formula de Ross-Heidecke para cálculo de depreciación

1. FORMULA DE ROSS-HEIDECKE

D =	½(e/n+e²/n²) x Cnd x kc	kc = Factor de conservación
Cnd =	Cn - Cr	(según Tabla de Heidecke)
donde:		Datos:
e =	Edad de las construcciones	Año(s)
n =	Vida Útil Total (V.U.T.)	Años
Cn =	Costo Unit. de Rep. Nuevo (C.U.R.N.)	soles
Vr =	% de Valor de Rescate (V.Resc.)	0,0%
kc =	Factor de Conservación	0,9868
Cnd =	Costo Nuevo remanente a depreciar (C.U.N.R.) = Cn - Vr	
D =	Depreciación	

***Fuente**: Oré, C. (2019)*

4.1.7. Flujos Monetarios Netos

Un flujo monetario es todo costo o ingreso que acontece como derivación de la disertación, establecimiento y maniobra de un proyecto, por ejemplo: la inversión inicial, los costos operacionales, los ingresos brutos, etc. Por lo tanto, para efectos de este estudio los flujos monetarios netos fueron calculados mediante la fórmula siguiente:

$$\mathbf{imin} = [\mathbf{id}(\%) \times \mathbf{CD} + \mathbf{ip}(\%) \times \mathbf{CP}] \div \mathbf{II}$$

Donde:

- i_{min}: Tasa mínima de rendimiento
- id (%): Costo de capital de deuda
- ip (%): Costo capital propio
- CD: Monto de la inversión inicial financiada con deuda
- CP: Monto de la inversión inicial en capital propio
- II: Inversión inicial

$$\mathbf{i(min)} = [(0{,}26 \times 46.484{,}92) + (0 \text{ x } 00)] \div 46.484{,}92$$

$$\mathbf{i(min)} = [(12.086{,}07) + (0)] \div 46.484{,}92$$

$$\mathbf{i(min)} = 12.086{,}07 \div 46.484{,}92$$

$$\mathbf{i(min)} = 0{,}26\%$$

En tal sentido, la tasa mínima de rendimiento es de un 0, 26% de acuerdo con los datos que se poseen, este resultado permitió calcular el valor presente neto (VAN) y la tasa interna de retorno (TIR) como se presentan detalladamente en la tabla:

Tabla 14. Valor presente neto (VAN) y tasa interna de retorno (TIR)

1	Datos para el análisis						
		importe					
	Inversión	46,484.92					
				AÑOS			
		inversión	1	2	3	4	5
	Flujo de caja (neto anual)	-46,485	47,414.62	48,362.91	50,316.77	51,323.11	53,396.56
2	Cálculo del V.A.N. y la T.I.R.						
		%					
	Tasa de descuento	0.26%	◄ Pon la tasa de descuento aquí				
	V.A.N a cinco años	202,346.06	Valor positivo, inversión (en principio) factible				
	T.I.R a cinco años	101.10%	Valor superior a la tasa, inversión (en principio) factible				
		ANEXAR LA MEMORIA DE CÁLCULO					

***Fuente**: Oré, C. (2019)*

Según el cálculo anterior, el valor presente neto es de **531.317,74** y la tasa interna de retorno de **155,33%** lo cual determino la factibilidad de la inversión, dado que el primer año de producción la empresa, tendrá una ganancia de doce mil ochenta y seis soles con ocho céntimos (12.086,08) gracias a la implementación del sistema de monitoreo lo que demuestra la viabilidad del proyecto.

En tal sentido, se presenta el cálculo del periodo de recuperación de la inversión el cual se efectuó mediante el cálculo de la variación acumulada del índice de precios de la empresa, la cual fue del 0,26%, considerando el crecimiento porcentual anual de la empresa-como puede verse en la tabla siguiente:

Tabla 15. Recuperación de la inversión payback

RECUPERACIÓN DE INVERSIÓN					
TMAR	PERIODO (AÑOS)	SALDO INVERSIÓN	FLUJO DE CAJA	RENTABILIDAD EXIGIDA	RECUPERACIÓN INVERSIÓN
26%	1	46484.92	-15507139.16	12086.08	-15519225.24
	2	15565710.16	-15467254.15	4047084.64	-19514338.79
	3	35080048.95	-15423805.42	9120812.73	-24544618.15
	4	59624667.10	-15373273.04	15502413.44	-30875686.48
	5	90500353.58	-15522211.09	23530091.93	-39052303.02
	6	129552656.60	-15258063.07	33683690.72	-48941753.78
	7	178494410.39	-15189156.79	46408546.70	-61597703.49
	8	240092113.87	-15113878.87	62423949.61	-77537828.48
	9	317629942.35	-15031488.58	82583785.01	-97615273.59
	10	415245215.95	-32274936.57	107963756.15	-140238692.72

***Fuente**: Oré, C. (2019)*

La tabla anterior muestra el periodo de recuperación en diez años de la inversión para obtener la rentabilidad exigida, menos el flujo de caja, permitiendo obtener la recuperación de la inversión en años la cual será de 33.683.690,72 soles en un periodo de 4 años, siendo rápidamente recuperada la inversión y con una rentabilidad en soles de 33.693.205,80 tan solo en 4 años a partir de la implementación del sistema de monitoreo.

4.1.8. Análisis de Sensibilidad del Proyecto

Los proyectos de inversión germinan como réplica a concluyentes insuficiencias humanas y su conquista estriba de la calidad de la necesidad a compensar. Esto, a su vez, es función del número de individuos afectados y del importe que éstas le asignan al efecto divisado. Desde el punto de vista empresarial, lo que importa es la posibilidad de que dicho valor

pertenezca a una explícita capacidad y destreza a pagar existiendo la generación de beneficios para financiar al menos los costos económicos.

De manera que la evaluación financiera de proyectos de inversión se entiende como el análisis que permite anticipar el futuro al identificar, medir y valorar la cantidad de inversión, ingresos, gastos, utilidad de la operación del proyecto de inversión, nivel de inventarios requeridos, capital de trabajo, depreciaciones, amortizaciones, sueldos, etc., a fin de identificar con precisión la rentabilidad y tomar la decisión final de invertir o no. Esto de acuerdo (Aguilera y Sepúlveda, 2005).

Este permitió valorar las ventajas y desventajas de la instalación del sistema de monitoreo, en cuanto al marco financiero, permitiendo identificar el rendimiento de la misma con una variación del 5% y del 1%, siendo la primera la máxima ganancia que puede obtenerse en esta empresa y la segunda la más desfavorable, estos resultados se presentan en las tablas siguientes a partir del ingreso bruto estimado para el primer año de operatividad:

Tabla 16. Variación de ingresos brutos en un 5%

Total de Ingresos Brutos en 5 Años					
Años	2019	2020	2021	2022	2023
INGRESOS BRUTOS	48.809,17	51.249,62	53.812,11	56.502,72	59.327,58
CRECIMIENTO AL 5%					
TOTAL, DE INGRESOS BRUTOS EN 5 AÑOS	2.324,25	4.764,7	7.327,19	10.017,8	12.842,66

***Fuente**: Oré, C. (2019)*

De allí que el total de ingresos brutos a partir de la variación de 5% será de 37.276,6 soles.

Tabla 17. Variación de ingresos brutos en 1%

Total, de Ingresos Brutos en 5 Años					
Años	2019	2020	2021	2022	2023
INGRESOS BRUTOS CRECIMIENTO AL 1%	46.949,77	47.419,27	47.893,46	48.372,40	48.856,12
TOTAL, DE INGRESOS BRUTOS EN 5 AÑOS	462,85	934,35	1,408,54	1.887,48	2.371,20

***Fuente**: Oré, C. (2019)*

De allí que el total de ingresos brutos a partir de la variación de 1% será de 7.064,42 soles. A continuación, se muestra la representación de los ingresos con variación del 5% y el 1% en la tabla 18:

Flujos Monetarios Netos con variación del 5% y el 1%

Habiendo calculado inicialmente la tasa de descuento la cual fue de un 26% y realizado el cálculo de valor presente neto y tasa de retorno con un crecimiento anual según del 2% anual en el ingreso bruto estimado, se procedió a realizar el mismo calculo suponiendo que el crecimiento sea de un 5% o de un 1%, lo cual permitió valorar las ventajas y desventajas del proyecto.

Tabla 18. VAN y TIR con variación del 5%

1	Datos para el análisis							información
		importe						
	Inversión	46,484.92						¿Qué poner aquí?
				AÑOS				
		inversión	1	2	3	4	5	
	Flujo de caja (neto anual)	-46,485	48,809.17	51,249.62	53,812.11	56,502.72	59,327.58	La tasa de descuento
2			Cálculo del V.A.N. y la T.I.R.					
		%						¿Qué es el VAN?
	Tasa de descuento	0.26%	◄ Pon la tasa de descuento aquí					¿Cómo se calcula?
								Análisis resultado
	V.A.N a cinco años	221,057.57	Valor positivo, inversión (en principio) factible					
								¿Qué es la TIR?
	T.I.R a cinco años	106.42%	Valor superior a la tasa, inversión (en principio) factible					¿Cómo se calcula?
								Análisis resultado
		ANEXAR LA MEMORIA DE CÁLCULO						

***Fuente**: Oré, C. (2019)*

Tabla 19. VAN y TIR con variación del 1%

1	Datos para el análisis						
		importe					
	Inversión	46,484.92					
				AÑOS			
		inversión	1	2	3	4	5
	Flujo de caja (neto anual)	-46,485	46,949.77	47,419.27	47,893.46	48372,40	48856,12
2			Cálculo del V.A.N. y la T.I.R.				
		%					
	Tasa de descuento	0.26%	◀ Pon la tasa de descuento aquí				
	V.A.N a cinco años	95,038.57	Valor positivo, inversión (en principio) factible				
	T.I.R a cinco años	85.77%	Valor superior a la tasa, inversión (en principio) factible				
		ANEXAR LA MEMORIA DE CÁLCULO					

***Fuente**: Oré, C. (2019)*

En tal sentido, si existe una variación del 5% o del 1% la realización del proyecto seguiría aun siendo factible, dado que si se incrementa es favorable y si disminuye aun supera la tasa de descuento, resolviéndose que la inversión será recuperada apropiadamente y según lo esperado. Por lo que para estar seguros de la sensibilidad presentada con una variación del 5% o del 1% se procedió a realizar el cálculo de la recuperación de la inversión, bajo la sensibilidad mencionada:

Tabla 20. Recuperación de la inversión con variación del 5% (payback)

RECUPERACIÓN DE INVERSIÓN					
TMAR	PERIODO(AÑOS)	SALDO INVERSIÓN	FLUJO DE CAJA	RENTABILIDAD EXIGIDA	RECUPERACIÓN INVERSIÓN
5.00	1.00	46484.92	-15507139.16	232424.60	-15739563.76
	2.00	15786048.68	-15467254.15	78930243.39	-94397497.54
	3.00	110183546.22	-15423805.42	550917731.09	-566341536.51
	4.00	676525082.73	-15373273.04	3382625413.66	-3397998686.70
	5.00	4074523769.43	-15522211.09	20372618847.16	-20388141058.25
	6.00	24462664827.69	-15258063.07	122313324138.43	-122328582201.49
	7.00	146791247029.18	-15189156.79	733956235145.90	-733971424302.69
	8.00	880762671331.87	-15113878.87	4403813356659.33	-4403828470538.20
	9.00	5284591141870.07	-15031488.58	26422955709350.30	-26422970740838.90
	10.00	31707561882709.00	-32274936.57	158537809413545.00	-158537841688481.00

***Fuente**: Oré, C. (2019)*

Tabla 21. Recuperación de la inversión con variación del 1%

RECUPERACIÓN DE INVERSIÓN					
TMAR	PERIODO(AÑOS)	SALDO INVERSIÓN	FLUJO DE CAJA	RENTABILIDAD EXIGIDA	RECUPERACIÓN INVERSIÓN
1.00	1.00	46484.92	-15507139.16	46484.92	-15553624.08
	2.00	15600109.00	-15467254.15	15600109.00	-31067363.15
	3.00	46667472.15	-15423805.42	46667472.15	-62091277.57
	4.00	108758749.71	-15373273.04	108758749.71	-124132022.75
	5.00	232890772.47	-15522211.09	232890772.47	-248412983.56
	6.00	481303756.03	-15258063.07	481303756.03	-496561819.09
	7.00	977865575.12	-15189156.79	977865575.12	-993054731.91
	8.00	1970920307.02	-15113878.87	1970920307.02	-1986034185.90
	9.00	3956954492.92	-15031488.58	3956954492.92	-3971985981.50
	10.00	7928940474.42	-32274936.57	7928940474.42	-7961215410.99

***Fuente**: Oré, C. (2019)*

Una vez realizado el análisis de sensibilidad se pudo determinar que aun y cuando el periodo de recuperación de la inversión tenga una variación del 5% y del 1%, el proyecto sería factible dado el total de recuperación, recuperándose para el primer caso en 2 años y para el segundo caso en tres años.

4.1.9. Análisis de Beneficios

A continuación, se presenta un análisis de los beneficios tanto tangibles como intangibles, que se pueden obtener poniendo en práctica la implementación del sistema de monitoreo haciendo uso del protocolo SNMP. Al momento de utilizar este sistema de monitoreo se generan ciertos beneficios como podrían ser:

- **Instalación del software de monitorización PRTG Network Monitor**:

  Se configurarán los diferentes tipos de sensores para cada dispositivo que se encuentre alojado en el Data center.
- **Cuentan con la más alta especialización profesional para desplegar todo tipo de proyectos:**

  Asumen todos los aspectos implicados en la detección de la problemática que presente el cliente, o reingeniería o adelanto de la Solución o Suministro de hardware y software o Establecimiento y

puesta en marcha o mantenimiento preventivo correctivo, monitoreo, administración, o simplemente capacitación.

- **Permite a los administradores de sistemas y redes obtener información:**

  Realizar lecturas de informes y gráficos de datos generados en tiempo real y periódicos, previsión de las tendencias de uso con el objetivo de optimizar la eficiencia del sistema de red y evitar posibles problemas.

- **Netsecure ofrece una solución de Monitoreo de Seguridad y Disponibilidad, en dispositivos críticos de su organización:**

  Brinda el acceso a una amplia y sofisticada gama de herramientas de gestión de la seguridad (SIEM) sin tener que invertir grandes cantidades de dinero ni tiempos de implementación.

- **Monitoreo 7x24:**

  Es un servicio primordial para lograr la continuidad operativa de su centro de datos, debido a que permite prevenir fallas y mejorar las operaciones.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. Al momento de realizar la revisión bibliográfica sobre el protocolo SNMP se realizó un aporte altamente significativo para conocer el mecanismo a través del cual se puede lograr información relevante de los dispositivos que hacen parte de la infraestructura de Netsecure Perú, obteniendo como resultado positivo el uso e implementación del mismo.
2. En relación al análisis hecho sobre las Aplicaciones de monitoreo más usadas en las empresas fueron concluyentes para establecer que el PRTG NETWORK MONITOR es el instrumento adecuado para ser implementada en la empresa Netsecure Perú, procediendo de un diseño práctico, configurable y escalable conforme a las necesidades de perfecciones de la red y los servicios ofrecidos por Netsecure Perú.

Recomendaciones

1. Como primer aspecto, se recomienda tramitar la mayor cantidad posible de dispositivos que acceden a la red y a los servicios de Netsecure Perú, de igual forma, de este modo se lograrán efectuar un proceso de Gestión de recursos y capacidades más eficaces.
2. Otro aspecto relevante seria actualizar persistentemente la aplicación en la medida que el distribuidor emita nuevas versiones más actualizadas, debido a que totalmente generan soluciones a inconvenientes que se muestran con las versiones presentes e ingresan nuevas funciones para perfeccionar la eficacia de experiencia observada por el consumidor final.

Referencias Bibliográficas

1. LEON, N. (2008). Gestión de la innovación tecnológica en el S. XXI. Documento disponible en: https://www.neuronilla.com/gestion-de-la-innovacion-tecnologica-en-el-mundo-empresarial-del-sxxi-neysi-ileana-leon-pupo/
2. TORRES, L (2017). Blog sobre Cómo optimizar el funcionamiento del Centro de Datos de su empresa. Disponible en: https://www.tkme.net/como-optimizar-el-funcionamiento-del-centro-de-datos-de-su-empresa/
3. El modelo ISO, (s/f). Documento en línea: http://www.exa.unicen.edu.ar/catedras/comdat1/material/ElmodeloOSI.pdf
4. PRGT Network Monitor, (2018). Disponible en: https://www.es.paessler.com/prtg/screenshots
5. PAESSLER, (2014). MultiSystem. Disponible en: http://www.multisystem.cl/productos/paessler/
6. Ley de Servicios de Seguridad Privada LEY Nº 28879 (2006). Disponible en: http://psm.du.edu/media/documents/national_regulations/countries/americas/peru/peru_law_on_pscs_2006_spanish.pdf
7. VALORADATA, (2018). Disponible en: https://www.valoradata.com/blog/importancia-de-la-contingencia-bcp-y-drp/
8. CEPAL, (2011). Sistemas aeroportuarios, servicio público e iniciativa privada. Disponible en : https://www.cepal.org/es/publicaciones/6356-sistemas-aeroportuarios-servicio-publico-iniciativa-privada
9. Saenz. A, (2012). El Éxito de la Gestión de Proyectos Un nuevo enfoque entre lo tradicional y lo dinámico. Disponible en: https://www.tdx.cat/bitstream/handle/10803/117483/Arturo_Saenz_%20Tesis_2012_Rev_1.pdf

10. Calderón. A, (2018). DISEÑO DE LA RED LAN DE LA EMPRESA ALTADIS FARMACEUTICA EN LA CIUDAD DE BOGOTÁ
11. Chicaiza. D, (2014). Estudio De Las Tecnologias De Seguridad Perimetral Informáticas Y Propuesta De Un Plan De Implementación Para La Agencia Nacional De Tránsito. Disponible en: http://repositorio.puce.edu.ec/bitstream/handle/22000/7896/9.56.000616.pdf?sequence=4&isAllowed=y
12. Arias, Fidias (2006). El proyecto de investigación: Introducción a la metodología científica. (5º. ed.) Caracas - Venezuela: Episteme.
13. Tecnologicon, (2015). Definiciones Básicas. Disponible en: https://tecnologicon.com/definicion-de-database-informatica/
14. Definicionesabc, (2012). Disponible en: https://www.definicionabc.com/ciencia/metodo-empirico-analitico.php
15. Aguilera, R. & Sepúlveda, F. (Junio, 2005) “Evaluación de proyectos de inversión para la toma de decisiones”. Economía y administración. núm 64, pp. 91-100, de http://www2.udec.cl/~rea/REVISTA%20PDF/Rev64/art5rea64.pdf